Unifying Cybersecurity:

Overcoming Fragmentation Through an Integrated Security Platform

Whitepaper

2024

AGILEBLUE

THE CURRENT STATE OF CYBERSECURITY

The 2024 global cybersecurity landscape is characterized by a complex interplay of technological advancements, emerging threats, and geopolitical dynamics. The digital ecosystem has become increasingly treacherous, with every company, irrespective of its size, being susceptible to cyber threats. Artificial intelligence (AI) and machine learning (ML) are pivotal forces shaping the cybersecurity landscape. While these technologies offer invaluable benefits in research and analytics, they also present new challenges as cyber adversaries leverage them for sophisticated attacks. The International Data Corporation (IDC) reports substantial growth in the AI cybersecurity market, indicative of the industry's reliance on advanced technologies. However, this positive trend is counterbalanced by the exponential rise in cybercrime costs, with predictions reaching $10.5 trillion by 2025.

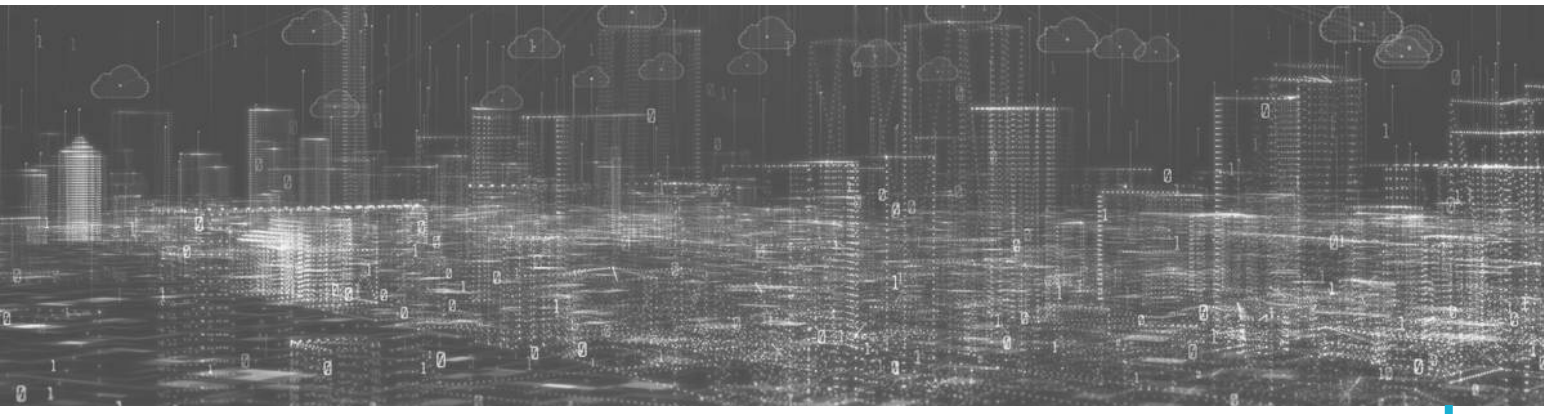
On average, organizations employ over

45 security monitoring solutions...

IBM, 2021

... yet **still face difficulties** in **attaining visibility** across various **tools** and **domains.**

Amidst this landscape, the stakes for cybersecurity have dramatically escalated, underscoring the need for a comprehensive approach to fortify organizational defenses. The scale of the threat landscape has grown exponentially, with cybercriminals increasing in number and organizational capabilities. The potential damage from a cyberattack looms as catastrophic, necessitating a reevaluation of cybersecurity policies. Information security faces challenges with the proliferation of data, posing privacy implications for customers and operational risks for internal workflows. Generative artificial intelligence (AI) further widens skill gaps within organizations, accentuating the urgency for an adaptive defense strategy. The adoption of consolidated security platforms emerges as a strategic imperative for enterprises to combat these issues.



Understanding Cybersecurity Fragmentation

Cybersecurity fragmentation poses a critical challenge in the modern digital landscape, characterized by the lack of integration and cohesion in an organization's cybersecurity measures. This fragmentation often results from the deployment of separate security solutions that operate independently, leading to inefficiencies in threat detection, response, and overall risk management. The absence of a unified and integrated cybersecurity strategy can leave organizations vulnerable to sophisticated cyber threats, as individual components may not effectively share threat intelligence or coordinate responses. One significant consequence of cybersecurity fragmentation is the difficulty in maintaining a comprehensive view of an organization's security posture. Siloed security tools and disconnected processes create blind spots, making it challenging for security teams to identify and respond to evolving threats in a timely and coordinated manner. This lack of visibility can lead to gaps in defense mechanisms, leaving critical assets exposed to potential breaches and exploitation.

of organizations are anticipated to **adopt a strategy unifying web, cloud services, and private application** access through a **single vendor's Security Service Edge (SSE)** platform by **2025.**

Gartner, 2021

To overcome cybersecurity fragmentation, organizations need to adopt a holistic and integrated approach to their cybersecurity measures. This involves implementing unified security platforms that facilitate seamless communication and collaboration between different security tools and processes. Standardizing policies and procedures across various departments and security teams helps create a cohesive defense strategy that can adapt to the dynamic nature of cyber threats. By breaking down silos, organizations can improve their ability to detect, respond to, and mitigate cyber risks effectively, ultimately fortifying their cybersecurity posture in the face of an ever-evolving threat landscape.

6 Benefits of an Integrated Security Platform

1 Unified Cybersecurity and Enhanced Productivity

Consolidated platforms offer a unified approach to cybersecurity, allowing the streamlined management of diverse solutions (e.g., patch management, threat prevention, privileged access management, etc.) from a single, integrated console. Automation features also simplify the tasks of IT administrators, boosting overall employee productivity and making the company more appealing to top talent.

2 Cost-Effective Centralization and Meaningful Insights

Choosing a security suite from a single Managed Security Service Provider (MSSP) eliminates the need for multiple vendor solutions, resulting in significant cost savings. Consolidated platforms also provide more meaningful and centralized insights, helping organizations fine-tune their cybersecurity posture and achieve a substantial return on investment (ROI).

3 Promotion of Business Agility

Consolidated platforms enable organizations to focus efforts on accelerating revenue growth rather than grappling with the repercussions of cybercrime. They also facilitate compliance with various regulations (e.g., GDPR, SOC 2 Type II, ISAE 300), providing a structured and efficient approach to meeting regulatory requirements.

4 Enhanced Defense and Attack Surface Minimization

An integrated security platform empowers IT administrators to stay ahead of emerging risks, resolve issues promptly, and improve incident response times. It also minimizes the attack surface by addressing digital and physical vulnerabilities, reducing the potential points of exploitation by unauthorized users.

5 Flexibility for Integrating Adjacent Technologies

Unified platforms offer the flexibility to purchase or develop adjacent technologies (e.g., Zero-Trust) and seamlessly integrate them into the platform. These integrated platforms also provide a comprehensive and adaptable defense against evolving threats, ensuring a proactive and dynamic cybersecurity approach.

6 Visibility and Reduction of Siloed Point Solutions

These platforms address the challenge of operating too many siloed point solutions, offering organizations enhanced visibility across tools and domains. They also mitigate the risk associated with adversaries thriving in the blind spots between security tools, providing a comprehensive view of the threat landscape.

43% of attacks are aimed at SMBs, but only...

14% of these businesses have the resources prepared to protect themselves.

TechTarget, 2023

COSTS SURGE WITH INCREASED COMPLEXITY

Insufficient integration among tools can pose significant operational challenges as your environment expands. With an increasing arsenal of tools, analysts spend more time familiarizing themselves with operations and correlating data to construct a comprehensive view of attack surface activity. This complexity amplifies with additional cycles needed for onboarding, training, and updating point solutions. The expanding toolset not only complicates deployment but also drives costs higher at every stage of the procurement life cycle.

Deployment Challenges

Introducing each new layer of protection can result in integration delays and the potential for "agent bloat," impacting endpoint performance. The cumulative effect of multiple tools during deployment increases complexities, leading to extended integration times.

Maintenance Struggles

Routine management transforms into a logistical challenge, frequently interrupting security operations. Coordinating each tool's unique update cadence demands continuous attention, including reboots, tuning, and reconfiguration.

Troubleshooting Complexities

Navigating a maze of vendors during incidents is hindered by the complexity introduced by multiple tools. Identifying blind spots becomes challenging, impeding the swift implementation of containment or remediation protocols. Limited integration across tools not only strains operational efficiency but also elevates costs, stretching resources across deployment, maintenance, and incident response stages.

277 Days on average for **security teams** to **identify** and **contain** a data **breach**. IBM, 2023

Consolidate Your Cybersecurity with the **Perfect Platform** for You

At AgileBlue, we stand as the **unrivaled choice** for organizations seeking to **elevate their cybersecurity defenses** through a consolidated and holistic approach. Our **Cerulean** platform, powered by **cutting-edge AI**, provides **unmatched capabilities** to detect cyber threats **faster** and **more accurately** across entire digital infrastructures. We take pride in offering a **comprehensive** suite of **services**, including **24/7 monitoring**, threat **detection**, and **response** capabilities, ensuring **potential breaches** are **identified** proactively and **mitigated** swiftly.

Our platform **seamlessly integrates** into **multiple layers** of your tech stack, setting a new standard for **precision** in today's cybersecurity solutions. What sets AgileBlue apart is our **commitment** to not just **monitor** and **detect,** but actively **manage** security **threats** through our **Managed Security Services**, tailored to your organization's **unique needs**. Cerulean combines **SOAR**, **SIEM**, **vulnerability scanning**, **24/7 incident response**, **XDR**, and **EDR** solutions—all **consolidated** into a **unified platform** that remains **unparalleled** in the industry.

In a league of our own, **AgileBlue** asserts its dominance as the **singular** and **superior choice for organizations** seeking not just a cybersecurity **solution**, but a **transformative** and **advanced** partner in **safeguarding their digital assets**. **Trust in AgileBlue**, where **excellence** meets **innovation**, and where cybersecurity is not just a service but a **commitment to unmatched protection**.

EMBRACE THE FUTURE.
SECURE YOUR PRESENT.

AgileBlue is proven to detect cyber threats faster and more accurately across your entire digital infrastructure and cloud. We provide 24/7 monitoring, detection and response to identify cyber threats before a breach occurs.

AgileBlue Cerulean is an AI-powered XDR | SOAR platform that automates the Security Operations Center with the human touch you trust. Our platform brings together cutting-edge machine learning, automated intelligence, and deep learning technology with the help of human expertise to tackle talent deficits, exhaustion, and ineffective methods within your organization. AgileBlue's Cerulean platform provides 24/7 monitoring, threat detection, cloud-based SIEM, and response to identify a breach before it occurs.

Ready To Start Protecting Your Company?

Contact Us