ePlus Solution Brief

Optimize Your Defenses

Consolidating and integrating security technologies.

Security platforms are increasingly becoming a core component to cyber security programs. Fragmentation in security tools and management consoles makes it challenging, if not impossible, to properly manage your security program and can increase your exposure to outside threats.

What is Platform Security?

Rooted in prevention, platform security refers to the security architecture, tools and processes that ensure the security of an entire computing platform and its associated applications & data. It uses a unified security software suite across hardware and virtual systems, on premise and multi-cloud environments and leverages defined processes to execute the mission of an organization's defined security program. Platform security is designed from the ground up to counter attacks before they manifest in an organization's environment. Platforms enable tasks that would formerly have had to be custom built into each system or application to be accomplished much more effectively by the reusable and integrated capabilities the platform provides.

Why Platform Security?

Security platforms must provide comprehensive coverage that includes endpoints and networks, as well cloud-based workloads and containers. A security platform must offer strong integration with and orchestrate behavioral analytics, vulnerability scanners, network admission control, threat intelligence, sandboxes, endpoint tools, incident response tools, and much more. Distilled down, it is the approach that brings together different cyber security tools into one unified system, helping you become more efficient and effective with your cybersecurity program. This has the added benefit of addressing many of the problems we face today, such as:

- Problematic cyber security skills shortage
- Tool and alert fatigue
- Evolving threat landscape
- Always-on business

How ePlus Can Help

ePlus provides technology and services to help you mitigate the risks associated with utilizing the multitude of disparate and burgeoning security tools that lack a common interface or integration method. We help navigate the sea of solutions and software to provide you an efficient, integrated and affordable solution. We work with your organization and understand the skills, processes and technology you have made investments in and will tailor our approach to ensure your organization is best positioned to mitigate this critical risk.

HOW CAN YOU ADDRESS THE CYBER SECURITY SKILLS SHORTAGE BY OPTIMIZING YOUR DEFENSES?

The cyber security skills shortage impacts organizations of all sizes, industries, and geographies. This means business leaders must consider these implications in every decision they make. Leveraging platform security allows sharing of threat intelligence throughout the infrastructure and offers unparalleled security across all networks, cloud and mobile.

- According to recent estimates, there will be as many as **3.5 million** unfilled cyber security positions by 2021.
- A recent ISSA study reported that **70 percent** of cybersecurity professionals claimed their organization was impacted by the cyber security skills shortage, with ramifications such as an increasing workload on cyber security staff and constant firefighting vs. proactive work such as planning, strategy and training junior staff.

CONTACT US

Contact us today to learn more about how ePlus can help you optimize your defenses.

@ eplus-security@eplus.com

☎ 1-888-482-1122

www.eplus.com/security

Where Technology
Means More®

THE EPLUS APPROACH TO OPTIMIZING YOUR DEFENSES

ePlus leverages partnerships with leading technology providers and couples that with our deep technical knowledge and experience to provide a comprehensive approach to creating the best security orchestration and automation architecture for your unique needs.

PREVENTION, DETECTION AND RESPONSE CAPABILITIES

Security platforms must significantly improve threat prevention when compared to running point tools stitched together. Each individual tool in the platform should offer a high level of security efficacy, while the platform should provide incremental threat protection as more tools are utilized collectively. Beyond threat prevention, each tool will also act as a sensor for collecting telemetry. The security platform will be back-ended by an advanced security analytics service that processes, analyzes, and acts upon this shared security telemetry. Security platforms must also offer well-defined and flexible options for responding to and mitigating threats, including automated and manual options. For example, the platform should automatically find and block retrospectively-installed files and indicators or compromise when new threats are detected in the wild. They should deliver, or offer options for, quarantining, deleting, or restoring data/systems/workloads to a known good state.

MANAGED SECURITY SERVICES IS A VIABLE OPTION

Once you have identified a security platform that meets your needs, you have addressed the technology portion of the people, process and technology triad. People and Process must also be considered for a holistic solution to exist. Building an information security program, measuring the controls put in place and managing vulnerabilities and business risk all require a variety of skills not typically possessed by a single individual, or multiple people at any organization. The required skills are hard-earned through a combination of years of experience and expensive training. By personalizing cyber security services to the top risks and compliance needs of your business, a **managed security services** provider can maximize your ROI while focusing on the most pressing risks and needs. A managed security services provider has **the people with the necessary skills and experience to help translate your business goals into effective security policies and controls** that will help mitigate identified risks. They can also deploy and maintain leading-edge, advanced security technologies that have been tested across many organizations in diverse geographies handling a variety of threats. This allows them to spread the cost of the experienced staff across multiple organizations. This economy of scale helps you to both save money, and get the necessary skills needed to run the advanced security technologies to protect your organization.

CENTRALIZED ANALYSIS AND MANAGERIAL REPORTING

In a security platform, all individual tools roll up to a **central management console**. The Integration of cyber security tools will enhance your ability to detect and respond to threats and improve the efficiency of security operations and analytics efforts. Consolidation and integration of security tools will allow for simplified cross-tool correlation and telemetry enrichment, as well as the chaining of individual events and adding context to data analysis. The integration of **intelligence analytics** will help reduce the burden on security staff, improve their ability to investigate critical alerts and decrease the amount of time for incident detection. It also enables the ability to identify threats across a broader range of your attack surface. The faster incidents are detected, the faster they can be responded to. This reduced time-to-detect minimizes the impact of a compromise or breach. Smarter alerts also ease effort required to prioritize events. As an added benefit, **role-based access controls** can be used to customize access for different users, views, and functions. Management data is also easily exportable to other tools if needed.

AUTOMATION, ORCHESTRATION & MACHINE LEARNING

Machine learning (ML) is already baked into security analytics. Marry the efficiencies of machine-speed analysis with the ability to react to approved events similarly through **automation and orchestration**, and you have achieved the reaction speed required to compete in the digital era. The future of cyber security is about humans and machines **working together to balance time and context**. Your security staff needs access to accurate intelligence rapidly, but they also need enough information to decide on how to act. For a routine procedure that is repetitive in nature, employing ML automates the decision process and greatly reduces time to action. Automated defenses are enabled through orchestration capabilities and advanced behavioral analytics. ML can also perform **predictive analytics**, which involves processing data and identifying patterns to make predictions and identify outliers. Together, ML, automation and orchestration can expedite and accelerate incident remediation. This improves security operations, enabling more value from existing tools and staff through greater emphasis on simplicity and efficiency. Also, **automating low-value, repetitive manual tasks can enable scarce, and over-burdened staff to focus on high-value activities**.

Cyber Security Frameworks

ePlus provides advisory services to help companies pursue alignment to leading industry frameworks such as CIS and NIST.

🟩 *Indicates control is either fully or partially addressed by this ePlus solution.*

CIS CONTROLS ADDRESSED

1	2	🟩 3	🟩 4	🟩 5	🟩 6	🟩 7	🟩 8	🟩 9	10	11	🟩 12	🟩 13	14	🟩 15	16	17	🟩 18	🟩 19	20

NIST CYBERSECURITY FRAMEWORK ALIGNMENT

IDENTIFY

ID.AM	ID.BE	ID.GV	🟩 ID.RA	ID.RM	ID.SC

PROTECT

🟩 PR.AC	PR.AT	🟩 PR.DS	🟩 PR.IP	PR.MA	🟩 PR.PT

DETECT

🟩 DE.AE	🟩 DE.CM	🟩 DE.DP

RESPOND

RS.RP	RS.CO	🟩 RS.AN	🟩 RS.MI	RS.IM

RECOVER

🟩 RC.RP	RC.IM	RC.CO

Corporate Headquarters:
13595 Dulles Technology Drive
Herndon, VA 20171-3413

Nasdaq: PLUS

©2019 ePlus inc. All rights reserved. ePlus, the ePlus logo, and all referenced product names are trademarks or registered trademarks of ePlus inc. All other company names, product images and products mentioned herein are trademarks or registered trademarks of their respective companies.