opentext™ | Cybersecurity

How cybersecurity platforms strengthen cyber resilience

Why simplification and vendor consolidation are now, more than ever, best practices to ensure cyber resiliency

What’s new in the ongoing debate between point solutions and integrated platforms?

Security professionals have a long history of debating the merits of point products versus integrated cybersecurity platforms. Many of the basic arguments haven’t changed. Backers of the “best in class” approach cite additional product features and very focused vendors. Advocates of integrated solutions point to faster deployment, easier management, and diversified, stable suppliers. Decisions still come down to the needs of individual organizations and the choices available in specific security domains.

However, recent trends have altered the balance of advantages for organizations that want to strengthen cyber resilience. Technologies like cloud computing, security analytics, and orchestration and automation, have had unequal impacts on the relative benefits of point products and integrated platforms. Developments in the business world, such as cyber insurance and the rise of managed service providers, also affect the comparison.

This white paper will review some of the longstanding pros and cons of the two approaches to acquiring security solutions. We will then examine how technology and business trends have changed the terms of the debate. The last section will briefly outline how the Secure Cloud platform from OpenText Cybersecurity illustrates the advantages of a single cloud-based platform.

What is cyber resilience?

“The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”

– NIST SP 800-172

Traditional pros and cons of point products and platforms for SMBs and enterprises

Cybersecurity organizations typically deploy and manage a legion of tools to protect against threats to endpoints, servers, networks, apps, databases, and other information assets. One recent survey found that enterprises in the US and UK manage an average of 76 security tools. Organizations with over 10,000 employees average 96. Even medium-sized businesses are estimated to use 50-60, and small organizations between 15 and 20.[1]

As new threats emerge and IT architectures evolve, security professionals have the choice of upgrading their security solutions and acquiring new ones based on two different philosophies. One is the "best of breed," multiple vendor approach. The other is selecting integrated platforms that provide a selection of integrated products across a specific domain. Each approach has what might be called "traditional" advantages and disadvantages.

[1] Panseer 2022 Security Leaders Peer Report; BizTech.com: Most Organizations Use Too Many Cybersecurity Tools

Traditional advantages of sourcing from multiple “best of breed” vendors

Two arguments in favor of the “best of breed” approach have remained relatively constant over time:

More features:
Organizations will get the most useful features by matching security offerings in each product category against a list of the organizations’ needs.

Committed vendors:
Suppliers that specialize in one or two product categories are very committed to those categories and likely to offer support and enhancements for the long term.

Traditional advantages of deploying platforms that include integrated tools

Advocates of integrated platforms have also raised several points consistently:

Out-of-the-box integration:
Security teams don’t have to spend time integrating the component solutions themselves or tinkering with the interfaces between them when one product or another is upgraded.

Streamlined configuration and deployment:
Less integration work, one or a few agents to deploy instead of many on endpoints and workloads, and a smaller set of tools for installation and configuration.

Consolidated management and reporting:
One or a few management consoles and reporting tools instead of many.

Faster detection and response:
Better data sharing saves time manually importing and correlating security data from multiple tools, so SOCs and incident response teams can identify and contain attacks faster.

Single source for procurement:
Dealing with one supplier saves time on performing vendor due diligence, negotiating contracts, and managing purchase orders.

Improved support experience:
Find support resources faster and eliminate buck-passing between support organizations.

Established, stable vendors:
Suppliers have a diversified selection of solutions and are less at risk of being squeezed by a rival or undercut by a “free” offering in one product category.

Those areas where platforms reduce staff work and outsource time-consuming integration and management tasks to platform providers have become even more important in today’s environment, where trained security professionals are very scarce resources best employed with strategic projects.

How advances in technology and best practices have changed the game

Cybersecurity is never boring.

New threats and attacker techniques emerge every day. IT architectures are evolving rapidly. Business and compliance requirements are shifting. And security frameworks and technologies are advancing to address changing conditions.

These challenges and opportunities have profound implications for the point products versus integrated platform debate.

Let's look at some of the key developments and their impact.

Security solutions hosted on the cloud

Security vendors are moving their products to cloud platforms for the same reasons that enterprises are migrating their applications: reduced operating costs, ease of access, better support for remote offices and workers at home, and increasingly powerful management and security tools offered by cloud platform providers like Amazon, Microsoft, and Google.

One effect of this trend is to make do-it-yourself integration harder. Organizations have a lot of control over applications running on servers in their own data centers, exchanging data with other applications on the same network. But they don't have the same kind of access and control to applications on cloud platforms, making it harder to integrate those applications.

Integration can be even more challenging when point products are running on different cloud platforms. What if vendors A and B are hosted on AWS, vendor C favors Azure, and vendor D has a deal to run its solution on Google Cloud?

And of course, it is not easy to today to find people with the right skills and experience to integrate and manage products on cloud platforms.

Under these circumstances, it is even more desirable than in the past to let the security platform provider take care of integrating tools with each other and with management services offered by the cloud platform companies.

Data sharing, data enrichment, security analytics, and AI

Security platforms often include integration that makes it easier to share and analyze information gathered by different security tools. This capability has always been an advantage for platforms over point products, and it has become even more important as cyberattacks have become more complex and sophisticated.

Advanced, multi-phase cyberattacks often can't be detected by the data available on a single workstation, server, or network. Instead, to identify and analyze attacks, data, and indicators of compromise (IOCs) must be collected from multiple security tools and correlated.

"Data enrichment" goes even farther by automatically retrieving data related to a detected IOC. For example, when an endpoint protection tool has a suspicious login attempt from a remote system, other solutions on the platform can compile contextual information for the SOC team such as the IP address the request came from, past malicious activity associated with that IP address, and other systems on the network that have received login requests from the same source.

Security platforms often provide built-in data sharing and data enrichment. They also build reporting and security analytics capabilities into their platforms and allow them to work with many of the individual security tools.

Organizations that deploy point products from multiple vendors typically have a very hard time implementing data sharing and enrichment if they can do it at all. This reduces their ability to identify and contain attacks quickly.

Enterprises and security vendors are starting to employ AI tools to detect patterns that indicate malicious behavior. This will magnify the benefit of platforms, because access to larger and larger collections of data make AI tools more and more effective.

Orchestration and automation

Security teams now face such incredible volumes of cyberattacks that generate thousands of alerts and gigabytes of security data every day. They increasingly rely on automated workflows to process this flood so they can triage alerts, detect attacks, and swiftly carry out actions to contain threats and remove vulnerabilities from hundreds of distributed endpoints.

Many of these automated workflows cross different security domains. For example, an endpoint protection solution might detect IOCs on endpoints, and automatically generate alerts for a SIEM. The SIEM, in turn, could use security orchestration and automation (SOAR) features to correlate information from different sources, eliminate false alerts, triage alerts, consolidate alerts into a smaller number of incidents. The SIEM would then automatically define remediation tasks and send them to the endpoint protection solution and other security tools so they could prevent the attackers from moving laterally and reaching additional systems.

A typical scenario might be an automated workflow where an endpoint protection tool detects malware on a workstation, then initiates a process where an XDR solution determines that the malware is communicating with an external command and control site and isolates the workstation to prevent data exfiltration.

Today, some cybersecurity platforms incorporate SOAR capabilities that help organizations eliminate slow and time-consuming manual workflows.

Compliance

Organizations are putting more and more effort into demonstrating compliance with security regulations – and recently with privacy requirements as well. A big part of that is documenting that security controls are in place and operating continuously, and that security data and audit trails are being collected and backed up securely and reliably.

Producing this documentation with point products can be extremely labor intensive because enterprises need to pull together and organize data from multiple sources. In contrast, security platforms usually make it easier to compile compliance-related information.

In addition, when an organization deploys a leading-edge integrated platform from a leading security vendor, auditors can see immediately that a layered defense strategy is in place that facilitates required best practices. To take one example, they can quickly establish that a unified backup and recovery strategy is in place for endpoints, emails, social media posts, and other key assets.

Cyber insurance

Cyber insurance is another hot issue today. Organizations of all sizes want to hedge the risk of catastrophic ransomware attacks, expensive breach notification requirements, and lawsuits from customers, suppliers, and other third parties injured by stolen information. However, because cyber insurance firms have been stung by unexpectedly large claims related to successful cyberattacks, they are raising the requirements that organizations must meet to qualify for policies.

Security platforms make it easier for enterprises to show that they meet policy and technology requirements and therefore qualify for a policy with reasonable premiums.

Access to shared services (cloud and professional)

The current generation of security platforms take advantage of the trend toward microservices and service-oriented architectures by allowing cloud-based services to interface with many security solutions through one API.

For example, the same threat intelligence feed or reporting tool can work with all the component elements of the platform. In contrast, organizations that depend on point products often find themselves working with multiple threat feeds and reporting products, resulting in more effort to learn and configure multiple solutions and to work with inconsistent data formats, report templates, etc.

Platforms also make it easier to source professional services that cover multiple security domains. Platform providers can often offer or recommend consultants and experts in fields like penetration testing, digital forensics, and regulatory compliance who are already familiar with the solutions in their platform. With point products, the security team might need to find multiple experts or wait for consultants to come up to speed on products new to them.

Managed Services Providers

The number of organizations utilizing the services of managed services providers (MSPs) and managed security service providers (MSSPs) is continuing to grow. Many small and medium-sized businesses rely on them to monitor and manage all aspects of their cybersecurity infrastructure. Large enterprises are increasingly using MSPs and MSSPs to outsource selected monitoring and management functions, allowing in-house security teams to concentrate on new technology and business initiatives.

Integrated security platforms provide huge advantages for MSPs and MSSPs. Many of them feature multi-tenant architectures, access controls, data segregation, and accounting and billing systems essential for providing services to multiple clients in a shared environment.

MSPs and MSSPs also need to be able to scale, from small clients to large ones, from a few clients to many, and from a limited number of security solutions to a wide range. Most platforms are built to scale in all these directions.

Strategic vision and future proofing

While point product vendors focus on their specific product niches, security platform providers are more likely to have a strategic vision that encompasses integration, automation, and emerging technologies and concepts. This gives customers an element of “future proofing”; they will be able to take advantage of innovations and new best practices without needing to manually integrate additional solutions into their infrastructure.

Secure Cloud: The cybersecurity platform from OpenText

The Secure Cloud platform from OpenText Cybersecurity demonstrates many of the advantages of a cloud-based platform described in this white paper.

It combines best-of-breed data security and data management solutions from OpenText brands such as Webroot, Zix, and Carbonite – and longtime strategic partner Microsoft – into one platform. OpenText Secure Cloud simplifies deployment, licensing, management, support, data sharing, reporting, orchestration and automation, compliance, and other activities we have touched on here.

Secure Cloud dramatically simplifies the work of protecting, managing, and governing business data across endpoints, email environments, collaboration tools, and more. As illustrated in Figure 1, it integrates tools across three critical domains:

- Endpoint, network, and email security
- Resilience, recovery, and compliance
- Microsoft's Cloud for Modern Work and more

Secure Cloud provides examples of many of the strengths of security platforms that we have been discussing. For example, it:

- Offers a central console to provide single-pane-of-glass visibility into malicious actions and security controls
- Employs predictive analytics and AI tools to enhance the threat detection capabilities of endpoint protection, DNS protection, email protection, and other security functions.
- Uses industry-leading backup, archiving, and recovery technology from Carbonite™ to protect and retain files, emails, social media posts, and other types of data.
- Integrates unmatched threat data and insights from BrightCloud® Threat Intelligence, including 80+ domain classifications.

In addition, Secure Cloud customers are in a position to leverage additional services from OpenText Cybersecurity that cover multiple security and compliance domains such as security awareness training, penetration testing, risk and compliance advisory services, digital forensics, and incident response.

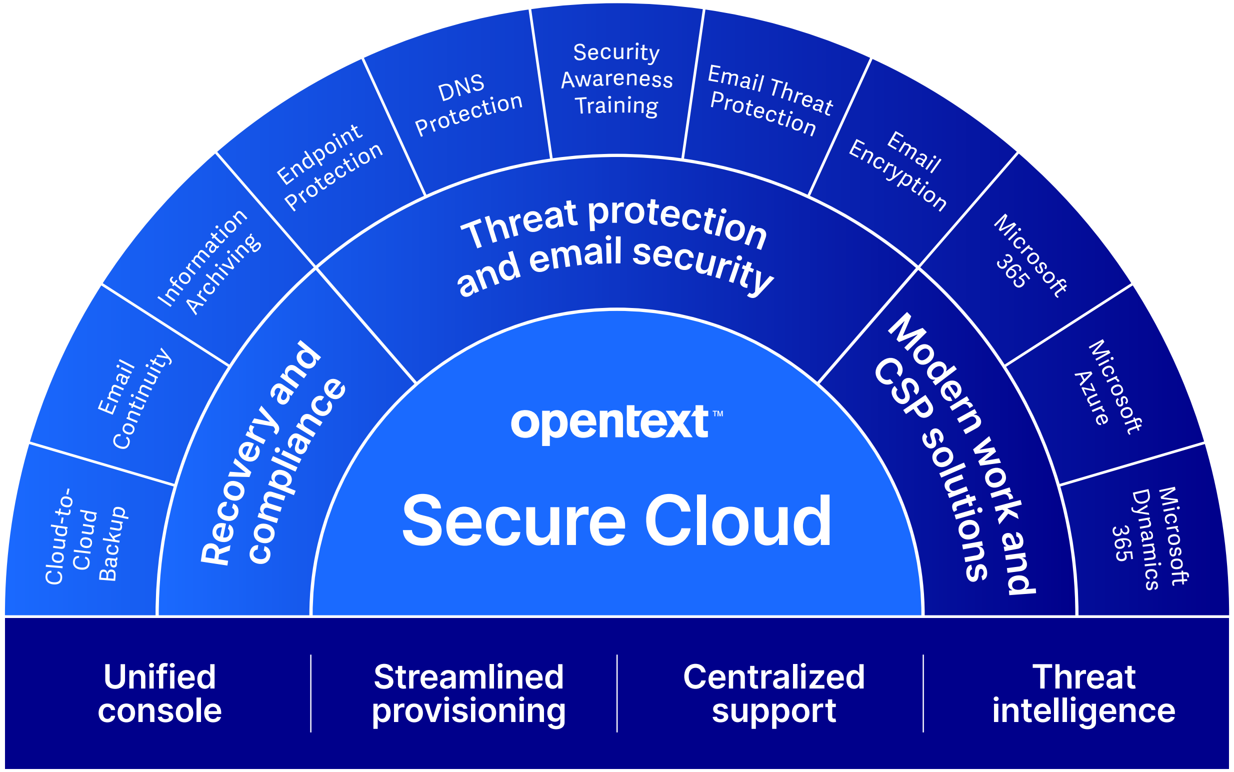

Figure 1: OpenText Secure Cloud integrates solutions for security, resilience, collaboration, and other domains

Conclusion

The debate between point solutions and integrated platforms isn’t new, but current technology trends and business developments have altered the discussion, as summarized in Tables 1 and 2 on the next page.

While there are still areas where a preference for point products makes sense, for security professionals, innovations in area like cloud computing, security analytics, AI, orchestration and automation, and services-based architectures have all moved the needle in the direction of integration and vendor consolidation. Business concerns such as demonstrating compliance with regulations and qualifying for cyber insurance add to the push in those directions.

In short, organizations today are likely to get much more value from working with security platforms and strategic suppliers who can exploit the power of integration, automation, and innovation across a range of security domains.

But don’t take our word for it. Come and see for yourself the power of an integrated security platform like Secure Cloud.

Traditional Pros and Cons	
Arguments for Point Product Approach	**Arguments for Integrated Platform Approach**
More features	Out-of-the-box integration
Committed vendors	Streamlined configuration and deployment
	Consolidated management and reporting
	Faster detection and response
	Single source for procurement
	Improved support experience
	Established, stable vendors

Table 1: Longstanding arguments for point products and integrated platforms.

Effects of technology and business developments	
Security solutions hosted on the cloud	Less access to software and solutions spread over multiple cloud platforms increases the difficulty of integrating and managing multiple point products.
Increasing benefits from data sharing and enrichment, security analytics, and AI	Cybersecurity platforms often build in data sharing and data sharing capabilities and provide simple access to security analytics and AI tools.
Security orchestration, automation, and response (SOAR)	Cybersecurity platforms often provide capabilities to orchestrate and automate workflows across security domains.
Compliance	Cybersecurity platforms reduce effort to create compliance documentation and implement best practices requested by auditors.
Cyber insurance	Cybersecurity platforms make it easier to show insurers that the organization meets policy requirements
Access to shared services	Cybersecurity platforms provide common access to technology services like threat intelligence feeds and reporting tools. Platform providers help source consultants and experts familiar with the platform and its components.
Managed service providers	Cybersecurity platforms often build in capabilities for managing multiple clients while ensuring security and privacy.
Future proofing	Cybersecurity platform providers continually incorporate emerging technologies and best practices into their platforms.

Table 2: How technology and business developments have changed the analysis.

For more information go to

www.webroot.com/securecloud

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. DS_071223