DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Qualys®

CYBERSECURITY CONSOLIDATION

Enabling a competitive edge and offering opportunities

DSCI-Qualys Point of View

Table of Contents

I

Current Digitalization Context

IDC estimates that digital transformation investment levels for 2022-2024 are expected to be $6.3 trillion and are 55% of all ICT investment by the end of 2024. The study further points out that for the first time ever, a majority of enterprise organizations (at 53%) have an enterprise-wide digital transformation strategy, a 42% increase from just two years ago. At the heart of this transformation lies the dire need to change.

Core operations:

- Transforming them from physical to digital by either reshaping the business model

Experience:

- Reconstructing the customer/partner and employee experience as a solid experience-feedback mechanism

IT infrastructure:

- Adoption of available cloud-based tools and new age technology stack to operate software, build and seamlessly integrate new applications, store/retrieve data, and compute

Data driven and analytics:

- Building a data-driven organization where decision-making relies heavily on insights obtained from gathered data

Culture:

- Drive culture change within the organization by integrating digital natives and immigrants to the digital era.

The onset of COVID has pushed the pace of digital transformation further ahead across the globe. The adoption of cloud computing, IT/OT convergence, IoT and IIoT automation, AI/ML, blockchain, quantum computing, AR/VR, and digital twins is on the rise. Technology integration and architecture up-gradation have opened the doors to a wide array of advanced cyber threats. The volume and velocity of data have increased exponentially with digitalization, necessitating the use of advanced cybersecurity systems to mitigate the risk of exploits such as malware and ransomware.

The need of the hour for enterprises as we exit this pandemic and prepare for a whole new world is business resilience and the ability to engage digitally with customers and within the company, which is propelling the global adoption and growth of the cloud ecosystem. Enterprises are experiencing a shift in business behavior, moving to cloud services from on-premises IT infrastructure and cloud migration has emerged as one of the major trends across several industries.

II

Modern Attack Surface

With digital transformation and the digitalization of existing assets, the risk of cyberattacks and associated risks such as data theft, ransomware, and operational disruptions increase. The attack surface also increases significantly, becoming more exposed. The modern attack surface encompasses the extended network of infrastructure, applications, endpoints, IoT, cloud, supply chain, and more, which all need to be protected. Moreover, to reduce threats to the modern attack surface, enterprises are leveraging advanced Attack Surface Management (ASM) tools and technologies. ASM enables enterprises to identify, classify, assess, prioritize, and oversee internal and external assets and data. ASM has emerged as a top priority for CIOs, CTOs, CISOs, and security teams, as several assets — known and unknown, rogue, and vendor assets — need to be protected to mitigate cyberattacks. Every day, millions of assets are exposed on the internet, unprotected by legacy firewalls and endpoint security technologies. ASM solutions include 5 major components

The attack surface is expanding and what is even worse is that about 30% of all on-premises and cloud assets are not inventoried. This is a key advantage for attackers to exploit.

ASM SOLUTIONS INCLUDE 5 MAJOR COMPONENTS

- Asset Discovery
- Inventory and Sorting
- Risk Assesement and Security Evaluation
- Security Monitoring
- Asset and Incident Monitoring for Malicious Assets

The attack surface within a modern IT infrastructure is huge and hyper-dimensional. Given the complexity of today's digital ecosystem, the challenges involved in attack surface management have increased significantly. If an unauthorized user gains access to an attack vector, it opens the door to data breaches or raises the risk of malware and ransomware attacks. Most enterprises have several attack vectors that might cause security issues and many lack the visibility or threat information needed to safeguard them. It's very difficult to prevent a breach without complete visibility into the various attack vectors that make up the attack surface. An advanced attack surface analysis allows security teams to have clear visibility into hybrid IT infrastructures and see it through the eyes of a hacker in order to improve the security posture. Attack surface analysis is an important tool for developing strategies for reducing the attack surface and identifying future threats that an organization may face.

ENTERPRISES CAN REDUCE THE ATTACK SURFACE BY THE FOLLOWINGS

- Minimizing Complexity
- Identifying Vulnerabilities
- Keeping Software Updated
- Controlling End Points
- Segmenting Netwoks
- Monitoring Active Domains and IP Addresses
- Prioritizing Remediation with Analytics

However, reducing the extent of the attack surface or the quantity of assets is not a robust solution, as a single vulnerability in any internet-facing asset can lead to an attack or data breach. Hence, enterprises need to have an advanced ASM solution to get real-time analyses of the attack surface and effective vulnerability management. Identifying points of exposure is the first step toward reducing the attack surface; having a detailed program to monitor and manage it can help enterprises avoid the most prevalent cybersecurity dangers that businesses face today.

HOW CAN WE PROTECT?

Web Applicataion Scanning and Firewall	Vulnerability Management	Patch Management	Cloud Security tools	*There are number of security solutions required and having several security solutions from different vendors may make it complex, so there is a need to consolidate the security*
Continuous Asset Monitoring	End Point Detection and Response	Compliance Tools	Threat Detection	

MODERN ATTACK SURFACE

Infrastructure	Applications	IoTs and IIoTs	Remote Devices	Cloud	Complex Supply Chain
Keeping unpatched Vulnerabilities	Network layer attack (DoS and DDoS)	Ransomware	Remote Access Trojans	Targeted phishing campaigns	Man-in-the-middle attack
Compromised and Weak Credentials	Malicious Insiders	Session Hijacking	Missing or Poor Encryption	Misconfigu-ration	Third and Fourth-Party Vendors	Unpatched vendor software

III

Complexity in Today's Network:

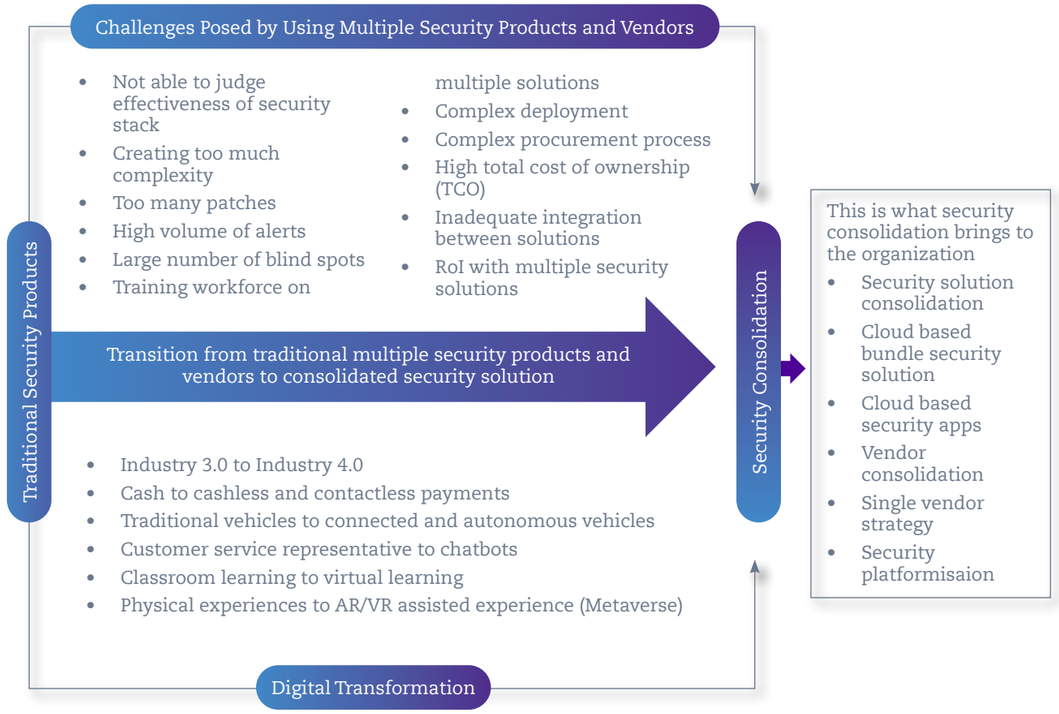
The Advent of Security Consolidation

Security consolidation has emerged as a major trend impacting enterprise security postures. Consolidation is a process of combining and integrating security tools and controls to reduce the complexity and effort required to manage the security infrastructure. Owing to the complexity in today's technology architecture/ infrastructure, enterprises are moving towards a centralized security management system, rather than having dozens of security products and vendors.

With multiple security solutions and vendors, organizations need specific skills to operate and maintain the security infrastructure. Also, there is a possibility of overlap across the tools and gaps in the deployed security solution. Today's hybrid IT environment and other components of digital transformation such as DevOps, which has seen a rise due to growing application development and modernization initiatives, require advanced security solutions to protect against threats.

> *"The security market is always consolidating but never consolidated."*
>
> *Bob Blakley, Former Gartner VP Distinguished Analyst*

The dynamic nature and changing landscape of cybersecurity has pushed large enterprises to deploy multiple security solutions from multiple vendors, which has further created the need for a multi-layered security architecture/ infrastructure approach. Multiple existing solutions can be replaced with more advanced, consolidated security solutions, which can enable the enterprise to reduce CAPEX/OPEX and complexity and increase efficiency.



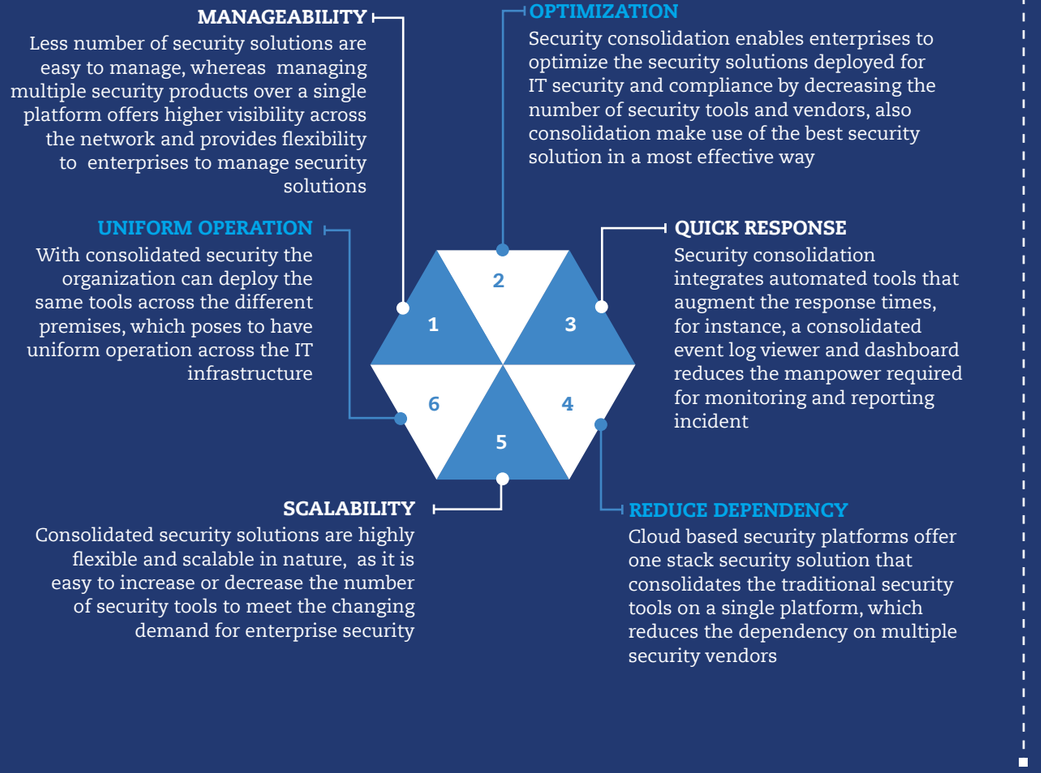
The ever-expanding attack surface requires advanced security defense systems which work beyond traditional security solutions to mitigate next-generation cyberattacks. The enterprise requires continuous monitoring of the threat landscape to prevent attacks on data and other systems. While consolidating, organizations should follow a holistic approach to cybersecurity and focus not only on reducing the complexity of their security solution but also on reducing risk.

On average an enterprise deploys more than 45 security tools on its network. Integrating more than 50 security tools leads to a less effective security defense system.

(Source: IBM)

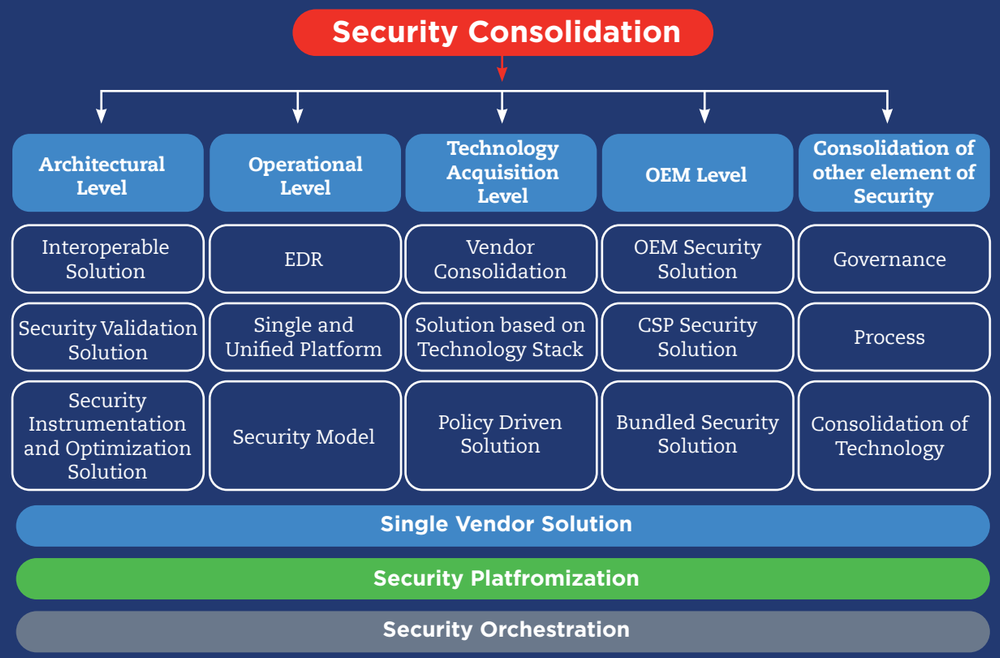
IV

Major Factors Driving Cybersecurity Consolidation



Dimensions of Security Consolidation

Security consolidation can be classified into several dimensions such as architectural, operational, procurement, OEM, and others. Apart from these dimensions, there are several ways by which security tools or the technology stack can be consolidated. There are benefits and advantages for every level of consolidation. For instance, consolidating governance and risk management enables enterprises to achieve GRC goals with better efficiency.



1. ARCHITECTURAL LEVEL

Security consolidation at the Architecture Level helps make security solutions more interoperable. In today's world of cyber-physical systems, CISOs are evaluated on their effectiveness, and, thus are looking for interoperability within the security solutions. Combining solutions such as cloud security, compliance, application security, network security, etc., will make the overall security architecture more interoperable and enhance the ability of security products to communicate with each other. Blending multiple cybersecurity tools and vendors creates interoperability complications, which in turn, weaken an organization's cyber defense system.

Integrating multiple security tools and making them work together has emerged as a major challenge for security teams. In many cases, some of the diverse security tools are unable to communicate with the platform, which slows down incident response and makes it impossible to get a holistic view of the threat landscape. To overcome such challenges, industry bodies and security providers are collaborating. In October 2019, for example, the Organization for the Advancement of Structured Information Standards (OASIS) launched the Open Cybersecurity Alliance (OCA) to create a standards-based, open ecosystem for building interoperable cybersecurity products without the need for any customized integration.

2. OPERATIONAL LEVEL

Security consolidation at the Operational Level enables organizations to leverage solutions with multiple security products such as threat detection, incident response, network security, log collection, analysis, and more. Consolidating multiple tools and capabilities on a cloud platform provides a cohesive and unified security platform. Operational-level consolidation enables an organization to run seamless security operations and provides many benefits, including lower CAPEX fewer training requirements, and licenses for multiple toolsets. Also, consolidation at the operational level reduces operating costs by simplifying and streamlining alert mechanisms to minimize false alarms and alert overload.

3. TECHNOLOGY ACQUISITION LEVEL

The Technology Acquisition Level opens new avenues to consolidate based on procurement decisions:

- **Procurement from one vendor** - A single-vendor approach minimizes complexity and provides a reliable, smooth security operation environment as it streamlines operations within a single platform, cloud, or on-premises.
- **Procurement based on technology stack** - More and more security vendors are developing AI/ML, blockchain, and cryptography-based security solutions. Easy integration of new technologies within existing cybersecurity frameworks makes the overall security solution more reliable and efficient. For instance, using AI/ML to predict, detect, and block threats and analyze data traffic on protected endpoints to identify both known and unknown threats. AI and ML algorithms can also be trained to generate alerts for threats and help identify previously unknown malware.
- **Policy-driven procurement** - To mitigate risk, many organizations are making policy-driven procurement decisions, opting to integrate cybersecurity solutions that focus on compliance with regulations, standards, and policies that are relevant to their specific business needs.
- **Vendor-customer collaboration**- Another key aspect of security consolidation at the procurement level is "Vendor-Customer Collaboration"—to deliver effective security solutions by aligning solutions at the technical and strategic levels. A close relationship and collaboration between cybersecurity vendors and customer creates a significant value to the security solutions by working together to develop innovative new security products and also strengthen the capabilities of both vendor and customer by helping in cost control, process optimization, and product/service innovation.

Customers are entering into the partnership with cybersecurity OEMs as a part of the procurement process to enhance the visibility from both sides, as the collaboration allows customers to have visibility into the supply chain of the vendor. Cybersecurity OEMs are also looking forward to collaborate with the customers by making customers design partners and early adopters of the solution to carry out consumer validation, which helps vendors to shape (do changes/modifications) the products. This also helps security vendors to enter into joint engineering collaboration for a product/service to validate the product use cases (which may not come in a first version of the product) to achieve the product maturity stage.

4. OEM LEVEL

Consolidating at the OEM Level allows organizations to procure security from large vendors and Cloud Service Providers (CSP). Large OEMs offer consolidated or bundled solutions on a single platform. CSPs offer security solutions for infrastructure and cloud services to enhance the enterprise security posture. Cloud hyper scalers offer advanced security solutions, analytics and operations, resilience frameworks, web app, API protection, and more for cloud, on-premises, and hybrid environments.

VI

Key Elements of Security Consolidation

Using a diverse toolset can result in blind spots that make it difficult for the enterprise to identify vulnerabilities and detect threats. The multiple alerts that separate point products generate can overwhelm IT's ability to investigate any anomalies. To limit alert noise and false positives, most solutions require sophisticated rules, policies, and suppressions, which often let real threats go undetected. Platformization (i.e., an integrated platform) and cloud apps enable security tools to work together cohesively, communicating with each other and sharing data to better align security with an organization's objectives. Security solution providers are coming up with all-in-one solutions that include asset management, vulnerability management, threat detection, response and prioritization, and patch management. Security consolidation not only reduces cost and complexity, but also reduces the number of false alarms or alerts, enables a quicker response to threats, and increases the overall effectiveness of security solutions.

1. CYBERSECURITY ASSET MANAGEMENT (CSAM)

Asset management plays a crucial role in developing the overall cybersecurity strategies of the organization, which requires enterprises to have wide and deep visibility of IT assets in a hybrid-IT environment. Organizations are leveraging contemporary asset management solutions to integrate legacy systems into a single system of record and automate the asset lifecycle. Asset management includes a process of discovering known and unknown IT assets and getting near real-time visibility of on-prem and cloud-based devices and applications. This is done by the integration of multiple sensors such as scanners, cloud connectors, container sensors,

cloud agents, passive sensors, and APIs. Asset management tools are available on the cloud, which is easy to deploy and maintain, and scalable to millions of assets. Also, it gives a comprehensive view of IT assets, including hardware and software data such as firmware, operating systems, and apps, as well as user information.

Another aspect of asset inventory and asset management is 'Asset Discovery', which includes a process of cataloging all the organization's assets that also helps in the identification of active and inactive assets in the network. The tools/technologies that are utilized, evaluate asset clusters and find linkages between their consumption, the network, and devices. Taking a thorough inventory of the IT network is part of the IT asset discovery process, this helps in understanding hardware and software that's linked to the enterprise network which encompasses both on-premises and cloud-based assets, giving in-depth network visibility. Asset discovery assists enterprises in the following ways: enhancing the security, network's hardware, and software assets visibility, simplifying tracking and report generation procedures, etc.

An effective cybersecurity strategy requires a virtuous and accurate asset inventory. Several enterprises heavily invest in IT and OT-level cybersecurity solutions to create comprehensive asset inventory, which can be used to identify and mitigate cyber threats. Cybersecurity Asset Management (CSAM) is a cumulation of endpoint protection, vulnerability management, cloud security, incident response, continuous controls monitoring, and security policy enforcement. Security providers are coming up with cloud-based asset inventory tools/services, which keep a track of asset information in real-time and can scale to millions of assets. Organizations integrate CSAM solutions to continue inventory assets, apply business criticality and risk context, discover

security gaps such as unauthorized or out-of-date software, and thereafter respond with appropriate risk mitigation steps which decrease the 'threat debt.' This is done by numerous layers of in-context technical and business data to provide a security perspective of IT inventory that makes at-risk assets easier to see. Establishing a security posture requires an understanding of assets having particular security and monitoring technologies installed, and which do not. Through dashboards and health reports, CSAM solutions can track and detect a variety of security endpoints, highlighting the breadth of coverage and crucial assets such as missing installations.

2. THREAT AND VULNERABILITY MANAGEMENT (TVM)

Threat and Vulnerability Management (TVM) is a critical cybersecurity practice for identifying and fixing security gaps that might lead to cyber-attacks. New vulnerabilities are reported almost daily, which means that organizations need to patch their systems and reconfigure security settings/strategies all too often. A fully integrated vulnerability management solution enables the enterprise to identify, evaluate, remediate, and report security vulnerabilities on systems, software, and IT infrastructure. The process involves four key pillars: inventory management, patch management, vulnerability scanning, and risk assessment.

Some advanced solutions include vulnerability management, detection, and response, an "all in one" solution to locate, access, prioritize, and patch vulnerabilities in real-time. These solutions are the cumulation of asset management, threat and vulnerability management, threat detection and prioritization, and response.

Also, traditional solutions require multiple teams and process such as vulnerabilities identification scanning tool and patch management, which leads enterprises to deploy extra resources and bear extra cost, which result in delayed patching. This can be mitigated with the advanced cloud-based solution which prioritizes vulnerabilities based on real-time threats such as ransomware, active attacks, malware, etc. This is done by enabling near real-time visibility to IT systems that are vulnerable to the latest threat, as it assists enterprises in detecting threats and monitoring unusual changes in the network before they become breaches.

3. PATCH MANAGEMENT (PM)

Patches are used to fix bugs, performance issues, and security vulnerabilities in software and applications. Effective patch management requires the ability to continuously track every new release of a code change. However, having a large number of endpoints and devices make it difficult to track a large number of patches. To overcome this, enterprises are adopting cloud-based, consolidated, and automated pathmanagement solutions with zero-touch automation. Poor patch management can result in exposing data to malware and ransomware attacks.

Automated patch management helps IT teams minimize vulnerabilities and easily patch their systems, saving time and effort. It also ensures that servers and endpoints are updated on time, reducing the overall risk of exposure. Security vendors offer an easy-to-use and deploy a cloud-based solution to patch Operating Systems (OS), mobile devices, endpoints, and third-party applications. Automated patch management enables enterprises to scan for missing patches, download

patches from vendor sites, deploy patches to vulnerable systems, and report on the status of patch deployment.

4. ENDPOINT DETECTION & RESPONSE (EDR)

A growing number of endpoints (e.g., desktops, laptops, servers, IoT devices, and mobile) across the network has increased potential points of entry where cybercriminals can execute code and exploit vulnerabilities. BYOD initiatives owing to hybrid work scenarios have exacerbated the situation. EDR combines real-time data analysis and monitoring of endpoints with a rule-based, automated response, making it a critical tool for protecting endpoints. The primary function of EDR is to monitor and collect endpoint data, identify threat patterns, and respond to threats with the help of forensic and analytical tools.

The focus of traditional EDR was limited to detecting attacks at endpoints utilizing multiple point solutions with large incident response teams, which often resulted in false positives and negatives. Today, cybersecurity vendors offer new EDR solutions that eliminate false positives and prevent lateral movements within the network. Modern EDR enables the enterprise to detect and respond to attacks and breaches, all from a single, unified cloud-based EDR application.

Enterprises increasingly experience multi-vector attacks combining diverse hacking techniques. Accordingly, enterprises require multi-vector endpoint protection solutions, which integrate multiple layers of protection, combining rules-based (known malware) and AI-based (machine learning, behavioral analysis, exploit mitigation) approaches and techniques.

EDR with a multi-vector focus provides prevention, detection, and response across the entire attack lifecycle with built-in anti-malware technology. With multi-layered anti-malware, anti-phishing, anti-exploit protection, and application behavior detection, multi-vector EDR is a consolidated solution that helps organizations minimize the overhead of operating anti-virus solutions.

5. EXTENDED DETECTION & RESPONSE (XDR)

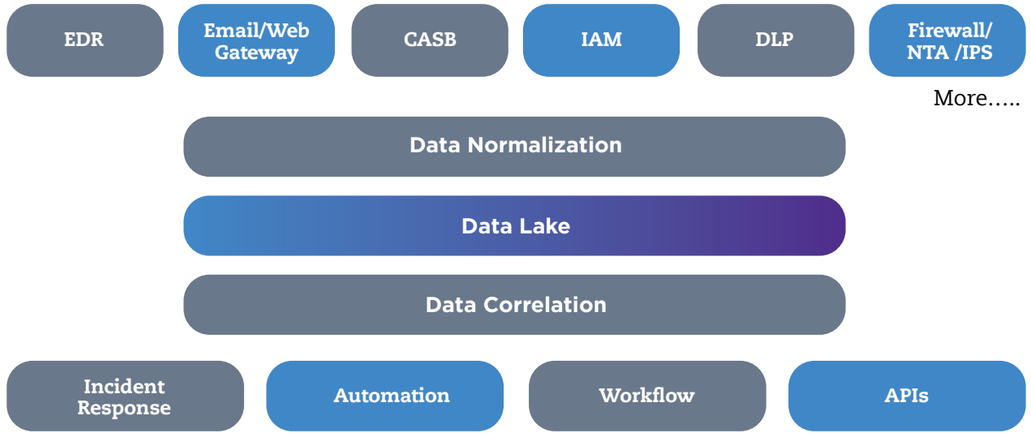
XDR is a SaaS-based security threat detection and incident response tool that integrates several security products/services into a unified security operations system. XDR enables enterprises to mitigate modern threats and attacks such as ransomware and zero-day attacks by implementing a proactive approach that includes prevention, detection, and response. Threat detection and response are made more proactive with XDR systems, as they provide visibility across

> ***Gartner predicts that by the end of 2023, more than 50% of enterprises will have replaced older antivirus products with combined endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions that supplement prevention with detect and response capabilities***
>
> *Source: Gartner*

all data sources, including endpoints, networks, and cloud data, and apply analytics and automation to prevent modern threats. XDR offers numerous benefits, such as improved protection, detection, and response capabilities, improved productivity of operational security personnel, and a low cost of ownership for effective detection and response to security threats.

XDR is a consolidation of multiple security tools in a single cohesive security platform to deliver enhanced detection and response results. XDR implementation combines and analyses data via a single lens, finding and correlating all relevant threats from data to provide a comprehensive evaluation of any possible threat. XDR incorporates sophisticated technology and applications that are intended to overcome the limits of EDR. It combines improved visibility across networks, clouds, apps, and endpoints with automated detection and response capabilities that respond rapidly to prevent both present and emerging threats.

Extended Detection and Response Conceptual Architecture



Source: Gartner

6. EMAIL SECURITY

The email security paradigm is changing rapidly. Organizations have continued to add several layers of security controls, as email attacks are becoming more sophisticated and targeted. Emails have been the most targeted or preferred path for the attackers to enter into the enterprise network owing to the growing email threat landscape. There has been a significant increase in the number of email attacks, the migration from traditional email to cloud email is pushing IT and security teams to re-evaluate their email security policies to ensure they are prepared to defend against the evolving threat landscape. Email security solutions help enterprises block advanced email threats such as malware, Advanced Persistent Threats (APT), phishing, spam, Business Email Compromise (BEC), and zero-day threats.

7. COMPLIANCE

Security governance and risk management is a process of continuous risk reduction and compliance with internal policies and external regulations like GDPR, CPI, and NIST. Modern governance and risk management solutions provide multiple compliance validations seamlessly. Compliance issues are recognized instantly and advised remediation measures are offered to the security team via a regulatory dashboard.

> *A strong consolidation, with a shift from best-of-breed players to well-established vendors will also be a key market trend in GRC software area.*
>
> *Source: Deloitte*

Achieving a unified picture of risk, compliance, and internal controls throughout the business is one of the primary Governance Risk Compliance (GRC) problems that risk and infosec professionals confront today. To accomplish this, businesses are moving away from a siloed approach and an integrated enterprise GRC program with well-structured and visible risk reporting frameworks, clear control systems, and streamlined information risk management processes, all of which can improve accountability and communication.

Complex environments like OT, IoT, and Quantum may expose the organization to third-party security and IT regulatory compliance issues. To centralize and monitor risk management while meeting compliance and reporting requirements, the organization must consolidate these touchpoints into a single GRC environment.

8. CLOUD / CONTAINER SECURITY

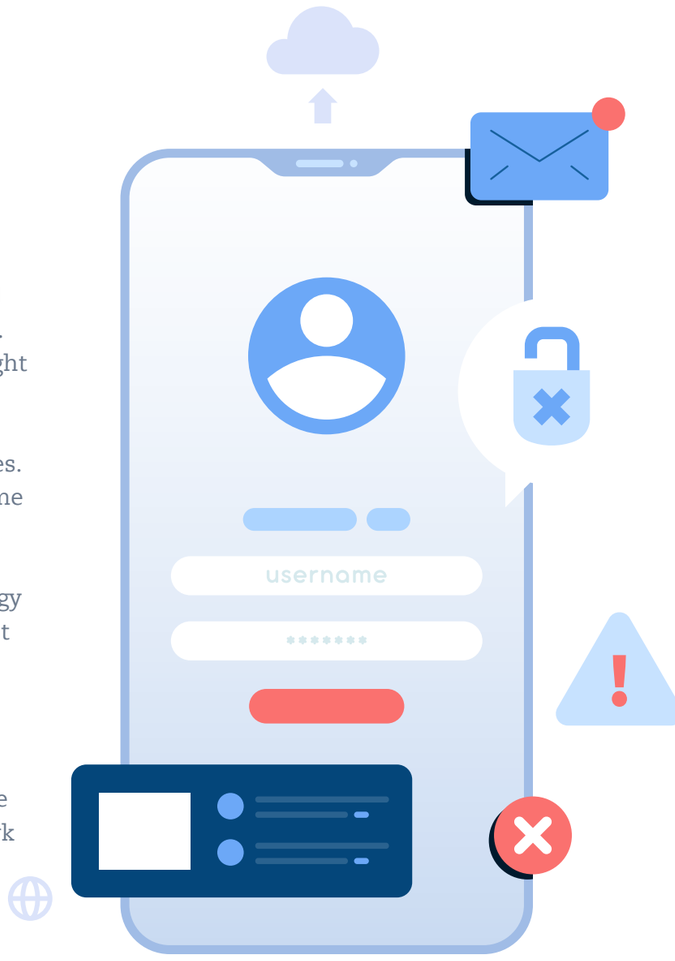
Cloud is one of the technological fields that has witnessed tremendous growth in recent years, and most enterprises are migrating from physical to virtual IT infrastructure to take advantage of cloud benefits. The necessity of the hour for businesses in the face of the epidemic is to connect digitally with their customers and employees, which has resulted in the cloud's rapid expansion. With the increase in cloud services and rising data storage over the cloud, security and privacy issues have been a key challenge for cloud users. Cloud provides several security benefits over on-premises, especially for smaller businesses, but only if cloud end-users avoid security mistakes such as misconfiguration, weak monitoring, poor patch management, weak authentication and authorization, and other security issues.

> *Through 2024, the majority of enterprises will continue to struggle with appropriately measuring cloud security risks.*
>
> *Through 2025, 99% of cloud security failures will be the customer's fault.*
>
> *Source: Gartner*

Today's enterprise operates several cloud services such as cloud apps, PaaS, IaaS, SaaS, etc. Cloud asset management is required by enterprises to track and maintain cloud assets. To have complete visibility and control of cloud assets and to deploy effective security and compliance products, enterprises need to have a comprehensive cloud inventory of public cloud workloads and infrastructure. This helps the DevOps team to continuously discover, track, monitor, and analyze cloud assets such as virtual machines, access control, storage, etc. in one place. The cloud asset inventory includes monitoring of cloud assets continuously, threat prioritization and insight, DevOps protection, quick identification of the incident cause, etc.

To build robust security for cloud assets and to protect from advanced threats, enterprises are including cloud security assessment into their cloud security strategy. This includes assessment and analysis of an organization's cloud infrastructure to ensure that it is secured against several security risks and attacks. This is done by providing actionable insight on misconfigurations and changes in security architecture to help enterprises prevent, detect, and recover from breaches. The cloud security assessment has become an important process of the overall cloud security, as it enables organizations to strengthen their risk management strategy and to establish a supported environment for being compliant with international regulatory requirements (GDPR and HIPAA). The cloud security evaluation helps to identify the organization's cloud infrastructure vulnerabilities and possible access points by investigating the network for signs of exploitation, and further outlining strategies for avoiding future attacks.

Enterprises are looking forward to having deep visibility and runtime application protection for server-based containers and Container-as-a-Service (CaaS) operating in a hybrid IT environment. Robust container security enables enterprises to leverage the benefits of cloud-native platforms. Also, the transformation of DevOps to DevSecOps — by integrating security into the initial phase of the software/application development to minimize the vulnerabilities, attacks, and downtime brings security closer to the containers. Container security solutions include discovery, inventory, near-real-



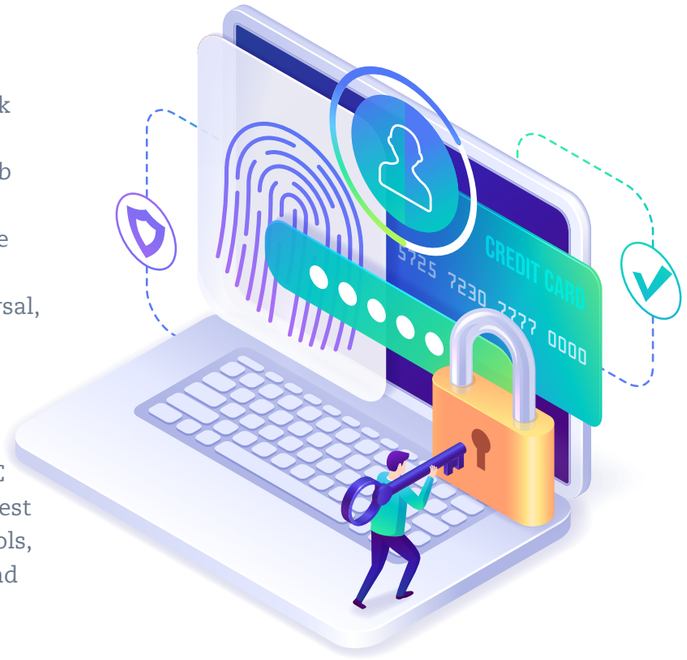
time tracking of container environments, vulnerability management, and compliance assessment. This is done by collecting and analyzing the inventory of images and containers, metadata information, event information, vulnerabilities, and compliance configurations with the help of sensors integrated with containers.

9. WEB APPLICATION SECURITY (WAS)

In today's world, most businesses run on the web and mobile apps. From personal entertainment delivery, e-commerce, internet banking, remote work applications, etc., the need of protecting web applications is the priority of enterprises. Web Application Security (WAS) or Web AppSec enables enterprises to secure websites and online applications from various security risks by integrating security controls into a web application to safeguard assets. A robust security strategy for web applications is critical for an organization to safeguard data, customers, and enterprises against data theft, business disruptions, and other losses due to cyberattacks. Web apps provide hackers with an appealing attack surface and a simple access point into an organization's IT infrastructure, if web apps aren't adequately secured. Most common web application attacks include SQL injection, XSS (Cross-Site Scripting), remote command execution, path traversal, Cross Site Request Forgery (CSRF), DoS and DDoS, etc. This can be mitigated by encompassing tools and technologies such as web application firewall (WAF), DDoS mitigation, DNS security - DNSSEC protection, encryption, IDAM, etc., and best practices such as automated security tools, cybersecurity framework, DevSecOps, and avoiding misconfigurations.

Web application scanning tools help enterprises crawl, discover, and detect web applications from the internet and intranet, and scan them for vulnerabilities and misconfigurations by providing comprehensive, accurate, and scalable web security. This is done by sensors that provide continuous visibility and analyze data in real-time. Also, this helps in preventing blacklisting and brand reputation harm by using scanning technologies to proactively monitor websites for malware infestations and issuing notifications to website owners. Scanning tools facilitate the DevSecOps practice, as they integrate security into the development phase by detecting code security issues and generating reports.

Traditional firewalls, such as network firewalls and Intrusion Prevention Systems (IPS), are effective in preventing unauthorized traffic and ensuring network security. However, they are unable to prevent advanced attacks such as SQL injection, session hijacking, cross-site scripting, or application-layer attacks. In recent years, there has been an upsurge in the rate and effect of web application attacks, to defend this, today's enterprise requires a next-generation firewall. Web Application Firewalls (WAF) are another pillar for securing applications running over the web, which works by blocking cyber-attacks by creating a shield between applications and the internet, and virtually patch web application vulnerabilities. WAF secures organization web apps by filtering, monitoring, and blocking critical HTTPS traffic, as well as preventing unauthorized data from exiting the app. This is done by adhering to a set of policies (which can be customized based on the web app requirements) that define what traffic is malicious and what is safe. WAF can be delivered to the organization in the following forms: appliance-based firewall, software-based firewall, and firewall-as-a-service over the cloud (cloud apps).



Application Programming Interface (API) Security has become a must have a security solution for enterprises. API development has increased rapidly in recent years, propelled by digital transformation and the critical role APIs play in mobile and web apps, IoT, etc. API security has become a top priority for the security teams as with the increase in API usage, API attacks have become more common. API cyberattacks frequently result in data breaches, exposing sensitive medical, financial, and personal information.

Source: OWASP

10. IT/OT CONVERGENCE

IT/OT convergence provides a unique application of digital technology to accelerate industrial business strategies as linked to an enterprise's digital transformation. Today, global enterprise manufacturing firms are moving towards Industry 4.0 to unlock the potential of data from their IT, OT, IoT, supply chain, and production systems.

IT/OT convergence is a merger of IT systems (storage, computing technology, business application, data analysis, etc.) and OT systems (supervision, control, process equipment, etc.). Today's OT environments are increasingly adopting new advanced IT technologies such as virtualization, cloud, AI, agile DevOps, and UX/UI, which eventually entails the convergence of IT and OT systems. The IT/OT convergence enables digital transformation across industries by using fog computing to enable real-time decision making to reduce unplanned downtime by predictive maintenance, deploy wireless technology on the production floor, and secure interconnected devices/equipment. The convergence of IT and OT systems offers several benefits such as cost reduction, improved capabilities, and higher efficiency, however, with the integration, the connected OT system are exposed to cyber risk within their SCADA and ICS systems. As a result, OT and IoT systems required advanced security solutions to mitigate the known and unknown threats by implementing specialized OT security solutions, which enhance the visibility of the OT network.

VII

Vendor Consolidation

With rising digitalization, enterprise IT assets have increased significantly. CTOs/CISOs are looking forward to decrease the number of security tools and vendors by adopting an IT/cybersecurity vendor consolidation strategy. While enterprises prioritize best-of-breed security tools/technologies that can be integrated, they are also reducing the number of security vendors. According to the Gartner "2020 CISO Effectiveness Survey"[3], 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more security vendors. As more and more security tools come to the market CISOs are considering vendor integration and management, CISOs are evaluating their security portfolio to check if a consolidation plan or best-of-breed approach is the best option.

A large number of security vendors create complexity in security operation, gaps in overall organization security, and increased security headcount, which can lead to a cyber-attack. Vendor consolidation may make contract administration easier and lead to better cost savings, however, it also comes with some of the risks that come with depending on a single vendor such as vendor lock-in, security tools cost, etc. This can be mitigated by consolidating security vendors to secure more assets with fewer vendors, which offers several benefits such as reduced vendor overhead, improved risk posture through more coverage, and reduced staffing. Organizations are giving greater effort to vendor risk management to reduce these risks by examining each vendor's cyber supply chain, personnel background checks, and technical support skills.

80% of organizations are planning to adopt an active security vendor consolidation strategy now and in the future.

15% of all organizations report having reduced vendors in the past year.

Source: Gartner 2020 Security & IAM Solution Adoption Trends Survey

VIII

Security Platformization: A New Avenue for Security Consolidation

Consolidating security with the platformization of security tools is another key aspect of security consolidation at the architecture level. Security platformization is becoming increasingly important in the digital world, and it is profoundly changing how security is seen, understood, and implemented across industries and businesses. CISOs are looking forward to platformize enterprise security. Security vendors are coming up with cloud-based or on-premises security platform which includes different components of organization security and compliance on a single platform. The platform-based security approach enables organizations to optimize workflow management and provide end-to-end security to give a real-time, holistic view of the threat landscape by integrating several standalone security solutions into one platform.

In the fast-changing security ecosystem, enterprises are adopting security platformization to secure more with lesser complexities and to also have a continuous assessment of the security and compliance posture in a hybrid IT environment. Security platforms help to decrease operating expenses, enhance operational efficiency and precision, speed up response time to security changes while lowering overhead, improve corporate security, and ensure business continuity. A cloud platform reduces the difficulty of maintaining various security systems while simultaneously boosting security automation, efficacy, and proactivity. Cloud-based security platforms offer several benefits such as seamless scaling, easy scanning of global assets, no hardware required, highly secured database, etc.

Security platformization models are gaining traction due to their ease of deployment, agility (premises agnostic), and the ability to integrate different tools. The platforms emulate enterprise security as a service and can offer a wide range of services including, but not limited to: threat intelligence, red team services, breach simulation, IDAM, risk monitoring, and visualization, vulnerability management, incident response, etc.

With security platformization, there is no further need to deal with tools that don't connect, no more redundancies, false alarms, and unneeded complexity, as everything is handled by a single security platform. Single platforms don't have to cope with the inconsistencies that arise when numerous security provider products are used, each with its own detection, design, and warning systems, as security coherence is ensured by using a single vendor and single platform. Aside from the reduction in overall complexity, the ability to expand IT assets is the most significant benefit of a security platform. This allows enterprises to respond to changing demands and security concerns without having to invest in new security solutions that may or may not function with the existing framework.

In the coming years, multidimensional platforms will play a considerably larger role in overall organization security. By shifting from traditional security solutions to security platformization enterprises can have significant outcomes such as open architecture, orchestration, automation, cloudification, and seamless global operations.

Futureproofing Cybersecurity for the Enterprise

Cybersecurity solutions and security vendors need to be future-proof. With the growing digitalization across the globe, the number of devices, endpoints, and data generated/stored is increasing significantly, which has opened up new avenues for cyber attackers. To mitigate advanced cyberattacks, enterprises are looking forward to moving from a reactive approach to a proactive approach for securing their assets and data and protecting data privacy. Taking a proactive, forward-contemplating approach to cybersecurity will help the enterprise prepare for the unexpected. Understanding enterprise risk is a critical aspect of developing a holistic perspective of cybersecurity vulnerabilities. Going forward the biggest challenges for cybersecurity are humans, machines, and data. Consequently, to have a robust security strategy, enterprises need to work processes, and technologies, which will ultimately help them mitigate human errors and implement situational awareness and intelligence-driven defenses.

As a result of numerous cyberattack instances across the globe, becoming "cyber-ready" has become a top concern for CEOs and board members of companies of all sizes and industries. Currently, the technology sector is witnessing a lot of progress in terms of security being built into standard product offerings. Organizations are focusing on streamlining and consolidating their security operations. Security leaders manage dozens of tools, but they intend to reduce the number to decrease complexities. SaaS or cloud-based security apps/solutions will become the primary delivery mechanism and influence hardware adoption timelines. Also, security consolidation may save money, simplify things, and offer new opportunities for profit and efficiency. Many security teams are taking advantage of the security consolidation trend as they deal with the plethora of budget constraints and expanding attack surfaces. When enterprises adopt a comprehensive approach to security, the major focus is on lowering the total risk by closing gaps and consolidating products and providers. Every security tool and its advantages should correspond to a serious security risk in the framework. Furthermore, each tool should lower overall risk, demonstrate a quantitative reduction in risk, and be able to maintain that risk reduction.

> ***By 2025, 40% of Board of Directors (BoD) will have a dedicated cybersecurity committee overseen by a qualified board member.***
>
> ***By 2025, threat actors will have weaponized operational technology environments successfully enough to cause human casualties.***
>
> *Source: Gartner The Top 8 Cybersecurity Predictions for 2021-2022*

X

Innovation vs. Delivery

Vendor consolidation fuels a conflict with the best-of-breed solution approach and delivery vs. innovation. Security consolidation entails moving away from the best-of-breed paradigm, in which CISOs select a single product or a minimum number of products for specific demand or technological niche. The premise for vendor consolidation emanates from the need for better efficiency, improved cost savings, and the complexity associated with having point solutions. Having a consolidated network security solution is better than having multiple security tools for Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Network Intrusion Detection Systems (NIDS), and firewalls.

In many cases, security consolidation is excellent as it simplifies the security stack, reducing the need to have multiple vendors for a single purpose. However, organizations typically require different security capabilities for different domains. CISOs are looking for tools that can prevent, detect, and respond to cyber-attacks, and at the same time enable product consolidation and integration. Cybersecurity is ultimately an organizational effort, requiring all teams and technologies to collaborate effectively. As a result, security efficacy should be evaluated at both the product and infrastructure levels. Each security technology must be best-of-breed, while also working as a force multiplier by increasing overall efficacy. Procuring cutting-edge security systems may appear to be a wise investment, however, organizations need to have skilled IT staff to operate and maintain them. The simplicity of implementation, time to value, and ease of use are important factors that need to be considered.

Contributors

DSCI

Vivek Sarkale
Senior Consultant, DSCI

Aditya Bhatia
Senior Consultant, DSCI

Eshan Hira
Senior Analyst, DSCI

Charu Sharma
Assistant Manager
Communications, DSCI

Qualys

Debashish Jyotiprakash
VP Asia, Qualys

Bijoe George
Director-APJC Marketing, Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based security, compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. The Qualys Cloud Platform leverages a single agent to continuously deliver critical security intelligence while enabling enterprises to automate the full spectrum of vulnerability detection, compliance, and protection for IT systems, workloads and web applications across on premises, endpoints, servers, public and private clouds, containers, and mobile devices.

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together governments and their agencies, industry sectors including IT-BPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

Data Security Council of India

NASSCOM CAMPUS, 4 Floor, Plot No. 7-10, Sector 126 Noida, UP - 201303

+91-120-4990253 | info@dsci.in | www.dsci.in

DSCI_Connect | dsci.connect | dsci.connect

data-security-council-of-india | dscivideo