White Paper

Before and After Next-gen: Cybersecurity Considerations that Transcend Paradigm Shifts

By Doug Cahill, ESG Senior Analyst

January 2017

This ESG White Paper was commissioned by Trend Micro and is distributed under license from ESG.

Contents

Executive Summary 3
A Confluence of Computing Shifts 3
Modern Data Center Architectures 3
Hybrid IT and Hybrid Clouds 4
Cloud-native 4
The End-user Is the Endpoint and a Perimeter 4
Agile Methodologies 5
DevOps Delivery 5
IT-as-a-service 5
Resource-constrained Cybersecurity Initiatives 5
The Fast-approaching Future 6
Multi-clouds 6
True Private Clouds 6
Connected Devices 7
Containers 7
Attributes of Timeless Security 7
Intelligent 7
Efficient 8
Coordinated 8
Purposeful 9
Essential Common Controls 9
Discovery 9
Prevention 10
Detection 10
Threats of Known Provenance 11
Threats of Unknown Provenance 11
Aligning Detection Controls with Assets 11
Response 12
The Bigger Truth 12

Executive Summary

The concept of a paradigm shift has been used to frame the enormity of fundamental changes in IT and compute models, as has been the case with the web, the client-server model before it, and so on. What is notable about today's current state of computing is that there are *multiple* concurrent shifts, with more on the immediate horizon, all while IT and security professionals must still manage and secure legacy environments. Compounding matters is the rate of change, the sheer velocity at which organizations are adopting new architectures, as well as methodologies and IT business models. For example, according to research conducted by ESG, 62% of organizations that currently use SaaS report leveraging these services for the delivery of more than one in five of their applications, up from 38% in 2013.[1] The rate of adoption is driven by business models that necessitate agility and data analytics. There is no question that it is an exciting time for information technology, but concurrent shifts warrant a strategic perspective with respect to cybersecurity.

Some technologies are like fads—they come and go through an adoption maturation cycle—but others are timeless—they cross generations, and cultures, and never go out of style. The Beatles are still relevant and popular among virtually all generations, and many of us across the globe look forward to the every-other year cadence of alternating winter and summer Olympics. In a cybersecurity context, the need to secure the past, present, and future raises the question of how to realize a level of continuity that transcends change over time.

In a cybersecurity context, the need to secure the past, present, and future raises the question of how to realize a level of continuity that transcends change over time.

Legitimate businesses, organizations, and public sector organizations do not possess exclusive rights on new technologies. Bad actors (hacktivists, cybercriminals, and nation states alike) also leverage new compute environments for zero-day malware and exploit development, as well as attack vectors. Some have even embraced the as-a-service model in new variants of ransomware to streamline the extortion process. And adversaries also keep a foothold in the past by repurposing tried and true threats including weaponized content and attack methods such as spam emails containing malicious links.

Indeed, those protecting against compromises and those perpetrating the attacks live in the three time dimensions of yesterday, today, and tomorrow. Organizations should evaluate security systems that not only support legacy and new environments, but also have a history of being out in front of new technologies that enable organizations to remain secure as they move from the lab into production. This paper explores the meta trends that make cybersecurity increasingly challenging and offers considerations for the evaluation of effective and operationally efficient security systems that can transcend paradigm shifts.

A Confluence of Computing Shifts

New architectures, fundamental changes in how end-users compute, and the ever-evolving threat landscape create a need for IT and security professionals to retool to keep pace with today's challenges, and be ready for the future, while also managing preexisting environments. The following paradigm shifts, each of which are expansive and thus could warrant such a dedicated paper, create new risks by dramatically expanding an organization's attack surface area.

Modern Data Center Architectures

Data center architecture has evolved from the physical to virtual and now to software-defined. For servers, that has meant going from bare metal to virtual machines to API-driven elastic workloads, with each transition occurring faster than the last. But these are not wholesale shifts. While on-premises server farms are largely virtualized, legacy bare metal servers, many running UNIX-based database workloads, are still in production and often mission-critical to business operations. For

[1] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, to be published.

many organizations, new applications are developed, tested, and deployed on software-defined infrastructure, including the networking tier, with the ability to create micro-segmented networks based on logical groupings as an instantiation of the least privileged best practice of access control. These technologies must coexist in today's data center as the variety of delivery models do.

Hybrid IT and Hybrid Clouds

The need for speed (expressed in IT jargon as agility) is highlighted by the time to provision new environments that automatically scale up and down as the application demands. Multi-month lead times to provision servers and apps are no longer acceptable service level agreements (SLA) and sharply contrast the on-demand availability of cloud-delivered services. But going fast can seem antithetical to security best practices. The cloud-first strategic imperative employed by many companies to evaluate all new IT initiatives through a lens of cloud viability results in IT being tasked to manage and secure hybrid environments.

But going fast can seem antithetical to security best practices.

Even if organizations have not yet deployed production workloads to the cloud, they very well may have a development team testing in such environments and almost certainly use SaaS applications such that they are, by definition, in a hybrid environment. Very often, cloud services, SaaS applications, and infrastructure-as-as-service (IaaS) are used by departments and business units outside of the visibility of corporate IT. In fact, according to research conducted by ESG, 65% of survey participants stated that they aware of a significant or moderate use of "shadow IT" applications in their organizations.[2]

Cloud computing—SaaS and infrastructure—is more than a technology transformation. For many, the cloud is as much an economic transformation, since it has changed cost structures from capital to operational expenses, reducing initial spend, enabling more predictive budgeting, and aligning cost with the actual consumption of services.

Hybrid IT results in hybrid clouds comprised of disparate environments that increase complexity and expand the attack surface area. While the temporal workloads in such hybrid environments create their own challenges, preexisting servers and endpoints need to be proactively updated. This combination of on-premises and cloud-resident infrastructure, applications, and data assets changes the complexion of the perimeter and how security professionals should think about it. While today's network perimeter is less defined than that of traditional data centers, hybrid environments still have physical perimeters, as well as those that are more logical in nature.

Cloud-native

A number of newer brands that are fundamentally disrupting and redefining the business models of traditional industries on their way to becoming multi-billion dollar businesses have never seen the inside of a traditional data center. These companies have "skipped GO" with respect to the current definition of legacy systems, but they too operate in multiple time dimensions, just as those who operate their own data centers or co-location environments. Such cloud-native companies leverage automation as a standard practice, operate in a workload- and API-centric orientation, and require security controls that align with these foundational aspects of how they compute. These cloud-native companies are also often early adopters for the future technologies discussed below.

The End-user Is the Endpoint and a Perimeter

Models that define the stages of cyber-attacks, including Lockheed Martin's Cybersecurity Kill Chain, highlight the central role the endpoint plays as the entry point via which threats are introduced and the foothold from which attacks communicate remotely and move laterally to additional targets. Protecting endpoints from such infiltration has been greatly complicated by a multitude of factors, including end-user mobility, the use of multiple devices to access corporate

[2] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.

…knowledge worker mobility and their use of external services—email, web, and cloud apps—make the user, not devices, both the endpoint and a logical perimeter that needs to be secured.

assets, and the widespread use of cloud applications, email, and the web. Users are simply engaging in riskier behavior than ever, and, as a result, are targeted by attack methods that take advantage of these factors, including fictitious business emails that trick users into making payments and the ongoing evolution of ransomware extortion techniques. While hybrid clouds contain physical network egress points as a physical perimeter, knowledge worker mobility and their use of external services—email, web, and cloud apps—make the user, not devices, both the endpoint and a logical perimeter that needs to be secured.

Agile Methodologies

The way in which API-driven infrastructure is provisioned, managed, and secured is as fundamental a change as the underlying technology. And these methodologies are no longer exclusive to cloud-native organizations, as they are now being employed as approaches to plan, manage, and secure on-premises and hybrid environments.

DevOps Delivery

DevOps is the convergence of previously disparate IT functions, development and operations, intended to streamline the delivery of infrastructure and applications via continuous integration, delivery, and monitoring. Further upstream, agile software development is now being applied to other project teams as a way to iterate quickly, by incorporating feedback and breaking deliverables down to smaller tasks. DevOps and agile share the tenet of being responsive by moving fast, such that security is too often an afterthought or viewed as an encumbrance to speed. But new architectures, as well as new methodologies, provide an opportunity to move security upstream by incorporating it into agile-based planning and DevOps-based delivery, so that security is baked in, not bolted on.

IT-as-a-service

The role of the information technology function itself is also shifting, forced to adapt to the business requirements for on-demand, self-service provisioning and usage-based pricing and chargeback models. Shadow IT is a manifestation of the fact that end-users and business units are no longer willing to wait for IT to stand up a new application. The transition to IT-as-a-service, via which IT employs many of the aforementioned technologies and methods to meet the agile needs of the company with a utility-based pricing model, are often part of the transition to a hybrid IT model.

Resource-constrained Cybersecurity Initiatives

Due to the awareness of the threat landscape and its potential impact on loss of revenue, loss of IP, damage to brand reputation, and interruption of business operations, cybersecurity budgets continue to increase. Research conducted by ESG on the spending intentions of IT decision makers underlines this response, with 69% of respondents noting that their cybersecurity budget will increase year over year. However, executing on initiatives funded by budgetary increases is still hampered by a lack of resources. Cybersecurity was the top area in which respondents reported a skill set shortage, with 45% of organizations citing such a shortage of skills as problematic.[3] Those cybersecurity skills that are in greatest need of development are, not surprisingly, those required to secure the aforementioned technology shifts, as indicated by ESG research in which 52% of organizations stated they intend to invest in the cybersecurity skills of the existing team, making it the most-cited action that their organizations would take in regard to cloud security in the next 12-24 months.[4]

[3] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, to be published.
[4] Source: ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.

This dichotomy of cybersecurity initiatives being funded but not resourced has implications for cybersecurity solutions, since it suggests that they should offer appropriate capabilities and user interface experiences for different audiences, including:

- **Operations,** for whom ease of agent deployment and policy management are important.
- **SOC analysts,** who require robust investigative capabilities.
- **CISOs and executive management,** who are interested in risk-based reports and key performance indicators on critical assets.

The Fast-approaching Future

Additional technologies that will be highly impactful to security architectures are fast approaching, with some organizations already moving production workloads to containers, employing connected devices for business analytics, and more. For others, these technologies are in the planning, lab, and evaluation phases, as they are readied for production purposes. In all cases, their adoption trajectory is being accelerated by the same business drivers as the shifts discussed previously—speed and efficiency.

Multi-clouds

While the use of multiple SaaS providers is common, organizations are now leveraging multiple IaaS platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Compute Platform (GCP) for cost leverage and to take advantage of best-of-breed services. ESG research indicated the move to multi-clouds is well underway, with 41% of survey participants stating they have a multiple cloud infrastructure strategy.[5] Such additional infrastructure diversity increases complexity, further expands the attack surface area, and requires augmenting native controls with a centralized policy engine and control plane.

True Private Clouds

What constitutes a private cloud gets conflated with server virtualization since virtualizing infrastructure does yield agility and efficiency. But those who posit "I virtualize, therefore I cloud" do not take into account other immutable aspects of cloud computing. True private clouds are API-driven, software-defined, and based on a services-oriented architecture comprised of physical infrastructure owned or leased by a single tenant. Such software-defined infrastructure spans the stack from network to workload.

While public and private clouds share the same need for speed, private clouds are driven by the need for economies of scale, and, as such, true private cloud adoption is mostly seen at large enterprises that require appreciable on-demand scale. Some large SaaS properties that start out on public clouds choose to transition those parts of their stack that are especially resource-intensive to private clouds, as is the case with the use of object storage by enterprise file sync and share (EFSS) services. And some large traditional enterprises are skipping or minimizing the use of public clouds to go directly to private clouds.

The security considerations introduced by private cloud are similar but expanded to those of public clouds. All auto-scaling environments create the need to protect temporal resources from compromise. While the cloud service provider (CSP) is responsible for physical security, network security, and more, all the way up to the hypervisor, the customers—security agreements with co-location facility providers notwithstanding—own securing the entire stack.

[5] Source: Source: ESG Research Report, *2017 IT Spending Intentions Survey*, to be published.

Connected Devices

The commercial application of Internet of Things (IoT) devices is expanding with many based on data-driven business models fueled by telemetry from connected devices such as retail systems that provide customer loyalty metrics. IoT is also employed in verticals such as health care for clinical systems, transportation for self-service kiosks, SCADA/ICT systems in industrial environments, and video surveillance, in addition to consumer applications including the connected home and automobiles. These and other use cases will result in millions of new IoT devices coming online over the next few years, as indicated by ESG research in which 26% of respondents noted that they already have IoT initiatives underway and another 42% stated they will as well in the next 12 to 24 months.[6]

The sheer scale of the proliferation of connected devices represents a massive expansion of the attack surface area. But as witnessed in the Mirai botnet denial of service attack in later 2016, IoT devices can also be unwitting botnet members that perpetrate attacks. The fact that many IoT devices are often remote makes it difficult, if not impossible, to update them, creating a requirement for resiliency by designing security in at the manufacturing phase. Once deployed, the device as well as the gateway via which it communicates to associated services, and the back-end services, often cloud-based, also need to be secured.

Containers

Another manifestation of the move to microservices for speed and flexibility, containers will be to applications what virtual machines (VMs) are to servers. Breaking application stacks further down into independent pieces makes each vulnerable and will require a variety of security constructs. As is the case with VMs, the underlying host, as well as inter-container communication, will need to be secure. Since containers are, by definition, portable entities, security will need to travel with containers and also be applied at the source from which a container is retrieved. While containers are new, many of the same security principles and controls will apply.

Attributes of Timeless Security

Security solutions that transcend the technology shifts of yesterday, today, and tomorrow should be thought of as systems that are intelligent in their use of detection and prevention techniques to efficiently coordinate protecting an organization's attack surface area with a purposeful set of controls. Such a holistic security system will have the following attributes.

Intelligent

The broad range of both known and unknown threats from malicious binaries to file-less exploits requires not just the use of multiple, non-mutually exclusive techniques, but the intelligent application of those techniques at the right time. Such techniques include reputation scores, machine learning, sandboxing, and behavioral analysis with more computationally intensive techniques applied later in the process and thus against a smaller set of potential threats. Known good and bad files, URLs, and IP addresses can be quickly identified based on provenance-driven reputation ratings so that more intensive techniques such as a machine learning and behavioral analytics are applied to determine the trustworthiness of a smaller set of new and unknown entities. An intelligent security system will not just incorporate threat intelligence, but make such information contextual and thus actionable. A static list of known bad URLs, IPs, and files is temporal in that hackers obfuscate attack sources and employ dynamically generated algorithms (DGA) to randomize the IP address for command and control servers, making blacklisting such addresses ineffective. But indicators of compromise (IOCs) coupled with the detection of the tactics, techniques, and procedures employed by bad actors from sensors and logs can help determine if an attack is underway. Furthermore, intelligent cybersecurity systems will be provided by vendors with threat

[6] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, to be published.

research teams who employ proactive measures such as bug bounty programs to discover new vulnerabilities before hackers. Such techniques need to continually evolve to keep pace with the ever-evolving threat landscape. Intelligent also means being smart about how the solution is designed for operational efficiency.

Efficient

While efficiency is an aspect of the other attributes discussed in this document, the challenge of securing disparate environments from different generations with a shortage of skilled resources against motivated adversaries is such that efficiency warrants a headline on the billing of essential cybersecurity system attributes. Indeed, efficiency is a critical success factor and is realized in a number of tangible ways:

- Reduction in the number of point tools allows organizations to develop a core competency on systems versus tools and provides centralized visibility and control across disparate environments and asset types.
- Ease of deployment and management with automation via integration with deployment and orchestration solutions expedites coverage.
- Ease of use via intuitive user interface workflows allows for streamlined policy assignment and reporting.
- Expedited detection via the use of sandboxing can dramatically shorten the time to investigate an incident.
- Minimal agent footprint and low false positive rate ensures end-user productivity is not impeded.
- Low latency and network resilience with highly performant network-based security controls will not impact quality of services (QoS).

Security-as-a-service, or cloud-delivered security, offers compelling efficiency benefits by removing the need to deploy and manage on-premises management infrastructure.

Coordinated

Many security professionals have had to adopt a best-of-breed approach to threat protection across the confluence of paradigm shifts. The resulting set of point tools creates disconnected silos in which learnings from one environment are not shared with others, controls are thus not fully leveraged, and the use of multiple sensors and consoles creates operational overhead. These inefficiencies are in opposition to the need to reduce time to detection and remediation, critical in preventing incidents from becoming breaches.

Connected security controls expedite threat detection, prevention, and response, dramatically improving organizational security posture by coordinating both visibility into possible threats and the applications of controls to prevent them. Foundational to a coordinated solution to improve cross-asset security is centralized management that spans the attack surface area of users, endpoints, networks, servers, email, web, and cloud services. Coordinated end-to-end security enables multiple uses cases, including:

- Host to Network: The automated remediation response to threats detected on an endpoint or server communicating with a remote command and control server can include instrumenting a network-based control to close ports and disallowing the associated protocols to disable such communication.
- Host to Network or Cloud and Back: New and unknown objects on endpoints are submitted to a network or cloud-based sandbox for detonation and runtime evaluation. If deemed malicious, the sandbox alerts the endpoint to remediate as well as the centralized management server to update prevention policies on all connected systems.
- Network to Host: Threats detected on the wire with network-based IDS/IPS or malware detection systems (MDS) should trigger endpoint and server checks for the presence of the same, resulting in appropriate remediation steps.

- Bidirectional Threat Intelligence: The detection of new and previously unknown threats on a host or a network creates an opportunity to share such intelligence in near-real time with all subscribers via a cloud-resident threat intelligence service that aggregates and disseminates new threat indicators.

These use cases demonstrate both intra- and inter-organization benefits of coordinated security.

Purposeful

The computing attributes of certain assets vary greatly. End-user-operated endpoints experience a high rate of variability and change and are subjected to interaction with multiple external entities that can serve as an attack vector. Fixed function systems found in retail environments, for example, are just that, fixed—closed systems that do not change. Temporal cloud-resident workloads in auto-scaling groups differ from their static virtual machine or bare metal on-premises brethren in important ways—workload instances are immutable in that they do not change once deployed to production. And on the network, physical controls are manually managed while virtualized networks employ software-defined constructs to, for example, automate segmenting access to resources.

Purposeful security controls are those that seamlessly attach to the resources they protect so that their presence is transparent. These examples illustrate the need for applying purposeful controls optimized for a specific environment including:

- Endpoint security should be aware of end-user use of email, cloud applications, and the web by utilizing proxies and APIs as a means of filtering and intermediating such access.
- Fixed function systems and servers can be better protected via the default-deny approach of application control.
- Cloud workload security can be automated via integrations with DevOps tools so that the appropriate security policies, based on tags, are applied as part of the provisioning process.

In addition to aligning controls with the asset being protected, being purposeful extends to economics. Timeless security solutions will offer pricing models that align with an organization's expense model, whether they are treating cybersecurity as a capital expense by purchasing perpetual licenses, a subscription for a term license, or a variable based on the actual consumption of a security service. Economic considerations of purposeful security also mean leveraging existing investments via integrations with examples, including alert propagation to security information and event management (SIEM) consoles and orchestration platforms to initiate a workflow.

Essential Common Controls

Organizations charged with securing past, current, and future paradigms should evaluate security systems that embody these attributes and enable the implementation of a methodology based on the discovery of assets, reduction of the attack surface area via preventative controls, use of a variety of techniques to detect new and unknown threats, and automated response and remediation. Like the time dimensions discussed herein, a security system has, is, and will be based on the use of layered controls to protect against the spectrum of threats from zero-days, malicious binaries, file-less attacks, exploits, and privilege escalation. To do so, a security system will centralize management of the following controls via common control plane.

Discovery

While the oft used term "visibility" is arguably ambiguous, the adage "you cannot secure what do not know you have" aptly captures the need to fully understand one's attack surface area as it ebbs and flows. Discovery should not be thought of as a point-in-time static list of resources. Given the dynamic nature of today's compute models with the temporal nature of server workloads in auto-scaling groups, and unpredictability of day-to-day user computing behaviors, discovery needs

to be based on continuous monitoring to maintain a current asset inventory. The visibility provided by discovery must be contextual to be actionable. To drive policy off of such context, security systems should provide enriched data across the four Ws of policy:

- What assets are in use (users, devices, applications, and data), including metadata such as tags that denote the role of a cloud workload.
- Who are the users accessing these assets, including which groups a user belongs to in order to establish normal computing patterns and detect anomalous activity.
- When are assets being accessed, updated, and, in the case of data, shared.
- Where are these assets located, including from where users are accessing them, their physical location, and their logical location (i.e., development and test versus production workloads).

The more multidimensional and cross-generational an environment, the more important such context and currency becomes. Discovery is foundational to the following controls.

Prevention

Preventative controls have two essential roles in a cybersecurity system: to stop known threats from installing, executing, and propagating, and to do the same as new and unknown threats are detected by techniques discussed in the next section. Hybrid clouds and worker mobility require preventative controls be deployed in multiple locations, including on the wire, at the egress, on endpoints, and on cloud-resident and on-premises servers. Essential preventative controls include:

- IPS on the network and servers block malicious netflow traffic by network zone to prevent cross-network propagation. Contemporary approaches to IPS will employ machine learning to predict malicious network activity based on attributes shared with traffic patterns known to be malicious and will also be able to detect and take action on behavioral anomalies across the network and in the cloud, including lateral movement and other activities associated with cyber-attacks.
- Application and integrity control provides a deterministic, default deny approach for fixed function systems, servers, and some knowledge worker endpoints, by only allowing authorized software to execute and preventing unauthorized configuration changes. Controls for system lockdown are also appropriate for highly purpose-built and deployed IoT devices.
- Gateways and proxying of web, email, and cloud app access apply policies, including those associated with SaaS application usage.
- Data loss prevention and encryption protect data at rest and in motion with user-centric policies to govern how data assets are accessed, updated, and shared.
- Host-based firewalls restrict traffic to and from servers, protecting them against inbound threats such as denial of service attacks and preventing outbound communication to command and control servers.

Detection

Detecting known and unknown malware and exploits (i.e., file and file-less threats) requires the use of non-mutually exclusive static and dynamic techniques. Such an approach starts by arbitrating between the known-good and the known-bad, the white and black, leaving a set of files that require further inspection, the gray. The gray or unknown files, for which there is not a clear initial verdict, require the use of multiple detection techniques.

Threats of Known Provenance

Reputation-based threat detection filters out known threats while allowing the known-good, whether they are applications to be run, emails to be read, or websites to be visited. To cover this surface area, a reputation service must be cloud-delivered, integrate with the aforementioned preventative controls, and provide the following types of reputation ratings:

- **Email (IP) reputation** services will catalog the IP addresses for legitimate email servers.
- **Website (URL) reputation** services will prevent users from visiting websites known to be used to disseminate threats.
- **File reputation** will identify files that are trustworthy, as well as those that have been established as malicious.

Threats of Unknown Provenance

A security system should provide both static and dynamic threat detection techniques for before and during execution analysis. Machine learning, based on algorithms trained against massive corpuses of both known good and malicious binaries and network activity, learns the attributes, over time, that make such traffic and files trustworthy or not. As such, machine learning is predictive in that it can detect unknown threats by detecting whether there are attributes shared with other known threats. Machine learning is also adaptive in that as the algorithm inspects more traffic and files, it literally becomes smarter.

To detect the threats that have evaded the aforementioned checkpoints, behavioral analysis vets files during runtime and in-flight network traffic to detect activities associated with malware, advanced persistent threats, and exploits, including:

- System changes (e.g., registry, file system, and new processes) including the rapid obfuscation/encryption of files by an unknown process that could be indicative of a ransomware infection.
- Scripts that inject malicious code.
- Weaponized content that exploits an application vulnerability.
- Browsers exploits in websites that use Java and Flash, which can be protected against with emulation and algorithmic detection.
- Malware fragments and corruption of memory spaces utilized by legitimate programs, which can be combatted with memory inspection.
- Network connections to/from IPs associated with command and control servers.

Aligning Detection Controls with Assets

Detection controls should also be applied across endpoints, servers, the network, and the cloud, with examples including:

- **Server- and network-based IDS** detects suspicious netflow traffic that could include, for example, malware communication with a remote command and control server and the exfiltration of data.
- **Endpoint detection and response (EDR) sensors** capture the interaction of threats with system resources and external entities.
- **Sandboxing** technology for malware detection should offer the flexibility of deployment either on the network and in the cloud, keep ahead of bad actor detection evasion techniques, and provide the ability to run a set of configurations that emulate customer environments.
- **Virtual patching** utilizes IPS rules to detect and prevent the exploitation of known vulnerabilities to enable organizations to defer patching production environments.

Response

Time is of the essence when an attack has been detected and assets are at risk. Organizations that have employed a security system that employs sensors across their attack surface area to record activity are better positioned to expedite their response and remediation. Such an audit trail enables the forensics analysis of how an attack entered an environment, the actions it took, whether it moved laterally, and even who attackers were based on how they operate. In this context, EDR sensors not only detect threats based on IoCs and behavior, but also capture the timeline of an attack based on interaction with system resources. Such event recording for search and analysis of binary activity across endpoints and servers enables key response use cases.

- Initiate Incident Response Workflow: Such solutions will also initiate the orchestration of incident response via integration into the IR workflow platform to coordinate the cross-functional investigation of the incident.
- Automated Remediation: Security systems will allow for the automated response to remediate an incident such as shutting down remote communication via network controls or quarantining an infected system. EDR tools will also capture the pre-compromise "known good" state to which infected systems can then be restored.
- Update Policies and Configurations: And as attackers themselves innovate to circumvent controls, such an audit trail provides visibility into their evolution of tools, techniques, and processes. Analyzing and understanding the actual behavior of successful infections enables organizations to update policies and the configuration of security controls.

The Bigger Truth

It would be difficult to overstate the significance of the velocity at which computing is changing, from data center architectures to end-user behaviors. And as rapidly as many organizations are transitioning to API-driven, software-defined environments, many are still responsible for securing legacy architectures. At same time, the threat landscape is ever-evolving, driven by highly motivated adversaries seeking monetary gain, political leverage, and more. The time continuum of the past, present, and future architectures requires that organizations adapt to protect against emerging threats that put corporate assets and business operations at risk. To do so, IT and security professionals need a solution that meets the challenge and stands the test of time. Going about this slowly is not an option. Security systems that will prove to be timeless are those that smartly apply the right set of controls and coordinate intelligence and actions across environments effectively and efficiently.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.