What's Next for Next-Gen Antivirus?

The modern workforce has become a distributed workforce, requiring teams to rethink their approach to legacy endpoint security solutions that weren't built to secure endpoints beyond the corporate network. The sudden surge of remote workers combined with the increased complexity of endpoint attacks signifies a clarion call for SecOps teams to move beyond a traditional, siloed approach that doesn't provide the full telemetry needed for the visibility required for threat response. As a result, enterprise antivirus solutions need to be hardened to withstand the increase in attack sophistication and frequency.

The cybersecurity market has sought to meet the need for tools that can identify advanced, sophisticated attacks, allowing enterprises to investigate what occurred, track, get to the root cause, and remediate affected endpoints. These tools fall under labels such as "next-gen antivirus" (NGAV), "endpoint protection platforms" (EPP), and "endpoint detection and response" (EDR), each of which now frequently encompasses overlapping capabilities. Not only does this make it confusing to know where to invest, but none of these approaches has proven to actually deliver the security outcomes enterprises need. If EPP is not delivering prevention and EDR is not detecting attacks, nothing is delivering the response.

In this paper, we'll take a look at the specific capabilities companies need to protect their endpoints against modern threats. We'll also examine scalable strategies for deploying these capabilities to optimize SecOps workflows and security outcomes, both now and in the future.

Great Prevention Is Still the Foundation of Security

Adversaries are crafty, and the volume and variety of potentially vulnerable endpoints continue to grow. It may not be possible to block 100% of threats—certainly not without blocking benign activities and significantly disrupting business operations.

With that said, it must be understood that detection and response are futile without consistent, coordinated prevention. Even when EDR performs exceptionally well, it still detects attacks only after the damage has begun. Detection after an attack puts SecOps into a reactive posture, first catching up with the damage and then investing operational overhead to understand and assess it before finally expending resources to mitigate the damage. EDR is like a collision sensor that triggers an airbag: airbags save lives, but preventing the crash in the first place is even better. A prevention-first approach means implementing the security equivalent of collision avoidance and deterrence. The first step to great prevention is examining the way organizations address threats.

Top Three Requirements for Endpoint Protection

Attackers must complete a certain sequence of events known as the attack lifecycle to accomplish their objectives, whether stealing information or running ransomware. Nearly every attack relies on compromising an endpoint to succeed, and although most organizations have deployed endpoint protection, infections are still common.

Many advanced attackers today blend two primary attack methods: targeting application vulnerabilities and deploying malicious files. These methods can be used individually or in various combinations, yet they are fundamentally different in nature:

- **Exploits** are the results of techniques designed to gain access through vulnerabilities in an operating system or application code.
- **Malware** is a file or code that infects, explores, steals, or conducts virtually any behavior an attacker wants.
- **Ransomware** is a subset of malware that holds valuable files or data for ransom, often under encryption, with the attacker holding the decryption key.

Due to the fundamental differences between malware and exploits, an effective prevention approach must protect against both and includes the following capabilities:

1. Malware Analysis

Today's complex threat landscape—combined with the diversity, volume, and sophistication of threats in the modern enterprise environment—makes effective threat prevention challenging. This problem is compounded by the challenge of detecting never-before-seen malware and exploits in addition to identifying known malicious content.

To address these sophisticated, targeted, and evasive threats, endpoint protection must integrate with shared threat intelligence to learn and evolve its defenses. To that end, integrating cloud-based threat intelligence with endpoint protection enables deeper analysis to rapidly detect potentially unknown threats. Machine learning on the endpoint should be able to rapidly assess a file to identify suspicious characteristics as well as perform deeper dynamic analysis and bare metal sandboxing as needed to prevent even more evasive malware.

2. Ransomware Prevention

Although ransomware is not new, major attacks like the REvil ransomware attack on Kaseya VSA (see figure 1) or DarkSide's assault on Colonial Pipeline have shown that traditional prevention methods are ineffective against advanced ransomware. Attackers have evolved their approach and use of malware to become more sophisticated, automated, targeted, and highly evasive.

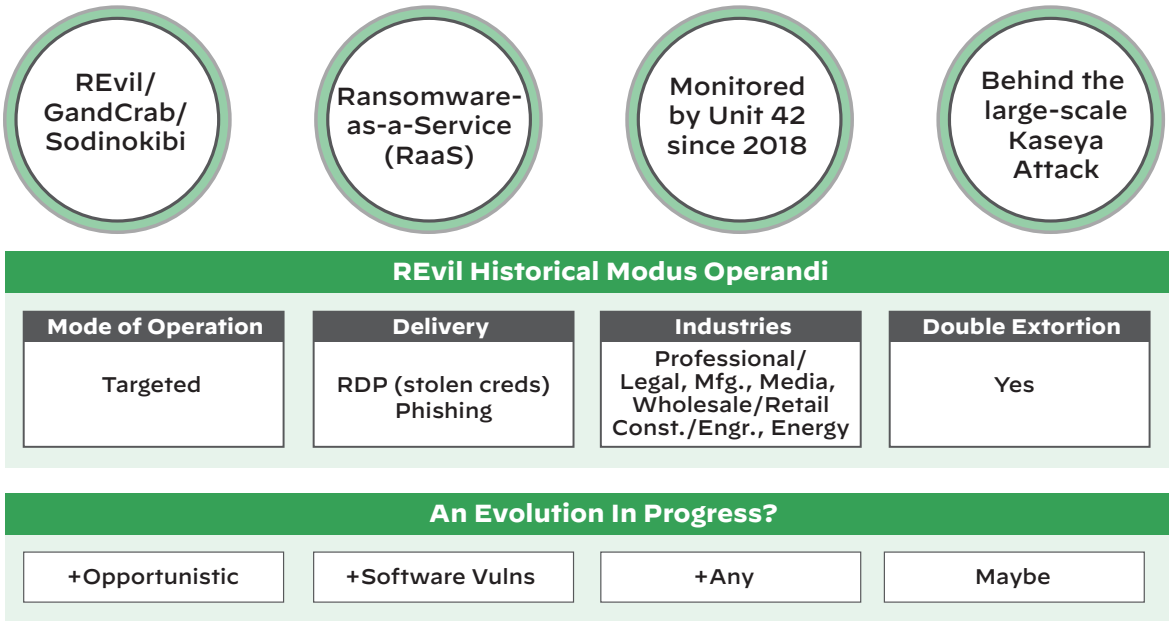

Figure 1: Unit 42 look at REvil ransomware attack on Kaseya VSA

Preventing ransomware requires a "defense-in-depth" set of capabilities on the endpoint to detect and shut down ransomware in multiple stages of the attack lifecycle. You would want **exploit prevention** to first detect the technique attempting to escalate kernel privileges to the user level and then shut down the attack. If that fails, **child process protection** should detect the parent process and stop it from spawning a child process. If those measures fail to detect the threats, the agent should be able to use **local analysis and machine learning** to identify the known characteristics of the malware.

3. Exploit Prevention

Thousands of new software vulnerabilities and exploits are discovered each year, requiring diligent software patch distribution by software vendors on top of patch management by system and security administrators in every organization. Addressing vulnerability exploits is the primary reason patches are applied.

Understanding Exploit Techniques

Many advanced threats work by placing malicious code in seemingly innocuous data files. When these files are opened, the malicious code leverages unpatched vulnerabilities in the native application used to view the file, and the code executes. Because the application being exploited is allowed by IT security policy, this type of attack bypasses application allow list controls.

Although there are many thousands of exploits, they all rely on a small set of core techniques that change infrequently. Regardless of the exploit or its complexity, for an attack to succeed, the attacker must execute a series of these core exploit techniques in sequence, like navigating a maze to reach the goal.

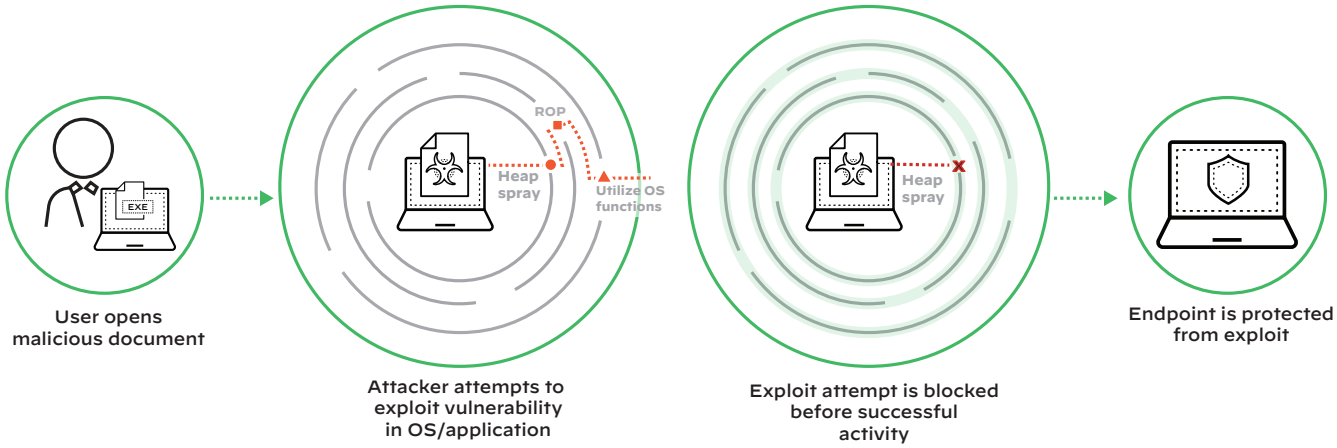

Figure 2: Focus on exploit techniques, not exploits themselves

Exploit prevention focuses on the core techniques all exploits use and, by rendering those techniques ineffective, negates application vulnerabilities whether they are patched or not. This approach is particularly critical for protecting heterogeneous environments—such as those with cloud workloads—where physical endpoint controls can create unforeseen complications in virtual environments.

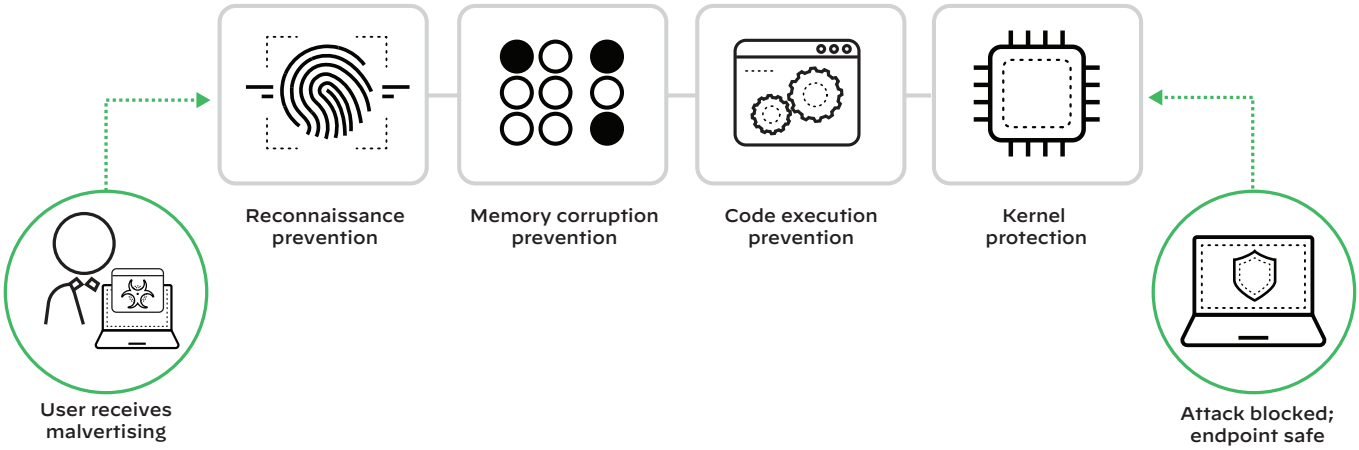

Figure 3: Multiple methods of exploit prevention

A Future-Proof Endpoint Security Strategy

While leading with great prevention is critical, it isn't enough on its own to defend against advanced adversaries. Your endpoint protection solution may block 98% of breach attempts, but that still leaves 2% that needs to be discovered and mitigated using detection and response capabilities.

These detection and response capabilities must extend beyond the endpoint—after all, adversaries don't stay on your endpoints, so why should your security tools? This is where EDR has failed, often leading resource-constrained security teams to waste hours following the breadcrumbs of malicious activity, only to find it was blocked by a firewall or other enforcement point.

Enter Extended Detection and Response (XDR)

It is better to deploy endpoint protection and detection capabilities as features of a holistic extended detection and response (XDR) platform that applies machine learning to a centralized data stream to provide full visibility into attacks across data sources and coordinate prevention across enforcement points. XDR takes prevention capabilities further than any NGAV or EDR, offering the full-scale visibility and powerful analytics that security teams need to fight sophisticated attackers now and in the future.

A 2020 study by Forrester Consulting shows that only 49% of organizations currently feel their various security tools are well integrated.[1] Organizations spend an inordinate amount of time getting the right data and making sure it's in the correct format to use for analytics. They may also need to collect data from multiple sources to determine which users, devices, processes, or applications are associated with specific events. XDR automates this through alert stitching—correlating related alerts from different data sources into security incidents—dramatically reducing the volume of disparate alerts analysts must face each day.

With lower alert volume, security teams can move much faster. Leading XDR solutions can close the security coverage gap through seamlessly integrated endpoint protection, detection, and response with a minimal footprint, no dependency on signatures for prevention, a cloud-based management interface, and extensive data collection for event and alert logging. This gives security operations teams the visibility they need for prevention-first operations without negatively affecting endpoint administration.

Your Next NGAV Investment Should Be XDR

Siloed tools and manual processes have no place in the future of security operations. Stopping sophisticated threats and their growing arsenal of tools will require much more intelligent and robust use of automation, big data, and machine learning, as well as a more integrated toolkit that allows for faster, more complete deployment of new features. Endpoint security investments should no longer be made solely based on the strength of the malware protection and the footprint of the endpoint agent but also with consideration for how they facilitate security operations workflows, which are crucial to an organization's overall security posture.

Consider new security investments based on the following capabilities and the ability to:

- Integrate protection, detection, and response controls, enabled by AI and machine learning that automatically seal the gaps.
- Unify controls that provide seamless communications between SecOps, endpoint and network administrators, and IR teams.
- Receive high-fidelity security alerts while reducing the "noise" from low-level alerts.
- Gain visibility across the entire infrastructure—endpoint, network, and cloud—to decrease detection and response times, thus driving down dwell time.
- Have validated third-party evidence to help inform threat hunting, namely integrations for the collection of telemetry and execution of response actions related to that telemetry.
- Gather and integrate deeply granular data from many sources, not just one.
- Run advanced analytics and machine learning on integrated data assets to spot malicious activities.
- Reduce investigation and response time by providing seamless visual interfaces that present an automated incident overview.

XDR is the only endpoint security solution that meets all these criteria. By combining rich network, endpoint, and cloud data with analytics, XDR speeds up alert triage and incident response, providing a complete picture of each threat and its root cause automatically, and reducing the time and analyst experience required at every stage of security operations, from triage to threat hunting. Tight integration with enforcement points empowers SecOps to respond to threats quickly and apply the knowledge gained to adapt defenses and prevent future threats, making the next response even faster. Moreover, as an added benefit, XDR further lowers the level of security analyst knowledge and skills required to respond to attacks, thus reducing the cost of security operations.

1. *The 2020 State of Security Operations*, Forrester Consulting on behalf of Palo Alto Networks, April 2020, https://start.paloaltonetworks.com/forrester-2020-state-of-secops.html.

Conclusion

By adopting a prevention-first approach with integrated protection, detection, and response, and by shifting the SecOps team's focus from "what" to "how," organizations are positioned to address four fundamental challenges: insufficient security, alert overload, siloed operations, and increasing dwell time.

Ensure you make your next endpoint security investment with this series of goals in mind:

- Integrate with all key security data.
- Eliminate low-fidelity alerts in the first place.
- Offer detection and response in a lightweight endpoint agent.
- Unify SecOps, endpoint administration, and IR via advanced causality chains.
- Deliver complete visibility across the entire infrastructure—endpoint, network, and cloud—to increase detection and response rates, ultimately driving down dwell time.

Deploy these capabilities in your organization, as specified, for optimal protection of your endpoints against modern threats, both immediately and into the future.

To learn more about XDR (Extended Detection and Response), visit our site.

Ready to begin modernizing your Security Operations Center? Download our white paper, *How to Plan for Tomorrow's SOC, Today*.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com