One Step Ahead of Adversaries

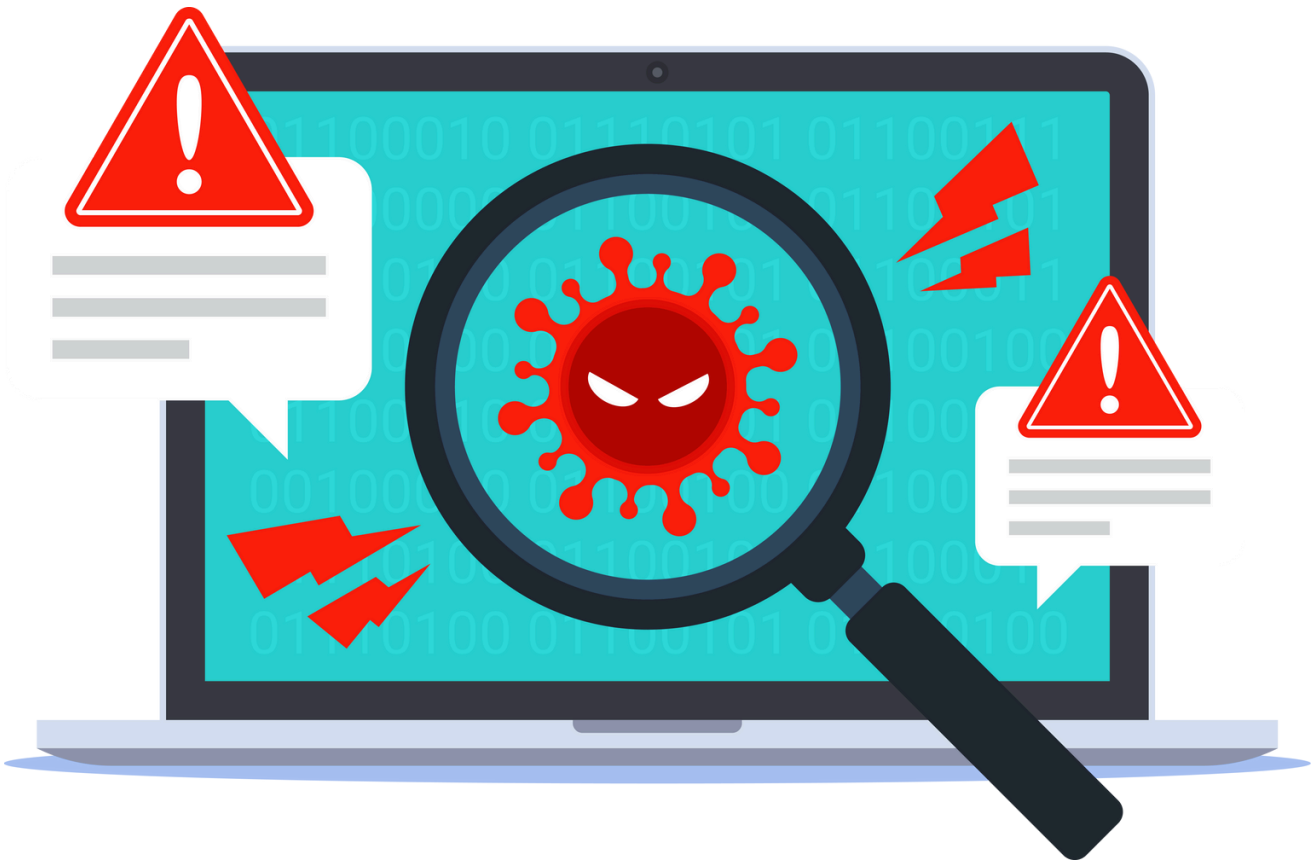
How Only a Three-level Technology Stack Can Deliver Complete Protection

Adversaries are smart, innovative, and aggressive – just like every cybersecurity vendor claims to be. But it seems that in most cases the adversaries are always a step ahead and vendors are playing catch up. On average, adversaries create 450,000 new pieces of malware every day. And a new ransomware attack occurs every 11 seconds. Yet vendors claim "world class" protection due to their innovation, use of AI, machine learning, and thousands of customers. Yet, those very same customers continue to experience breaches.

Are these technologies failing?

Are the adversaries that much smarter than your vendor? On the first I would argue, no – these technologies are doing exactly what they are designed to do. But on the second I would say "yes". Or at least the adversaries are smart enough (and motivated enough) to find the blind spots in legacy cybersecurity solutions – in particular endpoint detection and response (EDR).

The bottom line is, legacy EDR is designed to detect and block files, behaviors, and patterns that have proven to be malicious. But they are not, and never were, designed to address the new innovations that adversaries constantly introduce. Once a new threat (and there's 450,000 of them every day) is introduced and done its damage, then it becomes a known entity and can be addressed (or detected) going forward. But by then it's too late for the people already fallen victim to the threat.



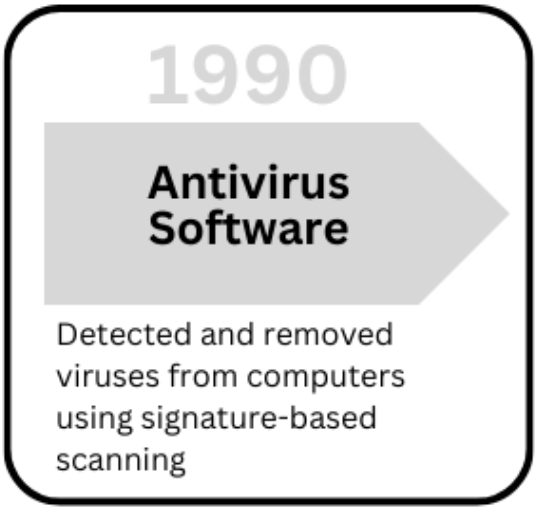
A Brief History of Cybersecurity

To better understand these blind spots let's take a brief detour into the history and evolution of the technology-stacks that have been built to combat adversaries.

A Deeper Dive – Three Level Technology Stack

In the late 1980s, the first antivirus (AV) software emerged to combat the growing threat of computer viruses. AV platforms were relatively simple, focused on detecting and removing known threats using signature-based scanning techniques.

We'll call this Level One of the technology stack.



Level One technology stack.

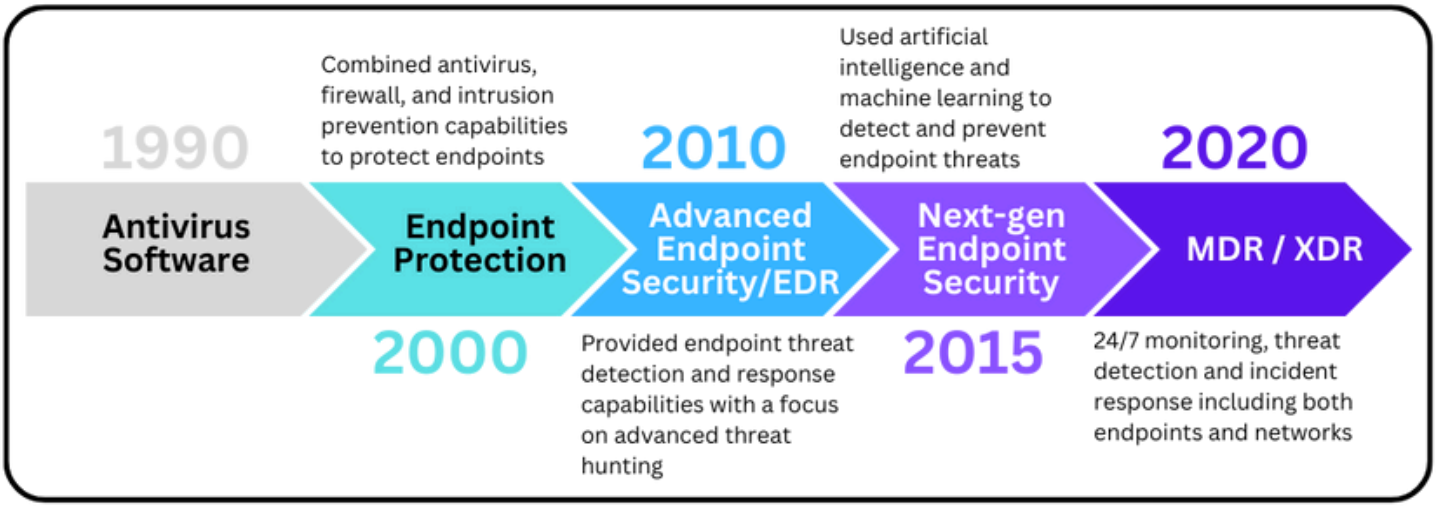
Detection:	Detects known malware by comparing files to a database of known virus signatures.
Threat Intelligence:	Requires periodic updates to keep the virus database current.
Deployment:	Installed on each endpoint.

Level Two – EDR to XDR

By 2010 adversary innovation to bypass traditional antivirus products, demanded more advanced protection. The response from cybersecurity vendors was the EDR platform. EDR platforms use behavioral analysis to detect anomalies and trace malicious activities across endpoints. This required a new technology stack running on the endpoint in addition to the necessary Level One technology stack. However, this approach has several limitations:

- It is still dependent on the solution's ability to detect the adversary's payload.
- The first attack will not be detected because it was an unknown entity (and therefore assumed to be safe)
- Since it is assumed safe, it is allowed to execute and inflict damage,
- Once a malware has proven to be malicious in someone's production environment will be added to the database of Known Bad and, after database update, be appropriately addressed going forward.

We'll call this Level Two.



Level Two technology stack.

Level Two naturally expanded to alleviate the burden of dealing with enormous amounts of EDR data and the resulting alert fatigue to offer cloud-delivered managed detection and response (MDR). In addition, the footprint of manageable and securable resources expanded to networks, cloud resources, and applications – extended detection and response (XDR).

Detection:	Real-time threat detection. Monitors endpoints, networks cloud resources, and more for behavior tied to known malicious activity. If a malware is not Known Bad it is assumed good and allowed to execute. Also includes threat hunting, behavioral analysis, and machine learning to expand the scope.
Threat Intelligence:	Collects data from multiple data sources and leverages global threat intelligence feeds.
Incident Response:	Provides tools to remediate when detection fails, and a breach/infection happens. Include security orchestration and automation
Deployment:	Centralized detection and analysis delivered from the cloud.

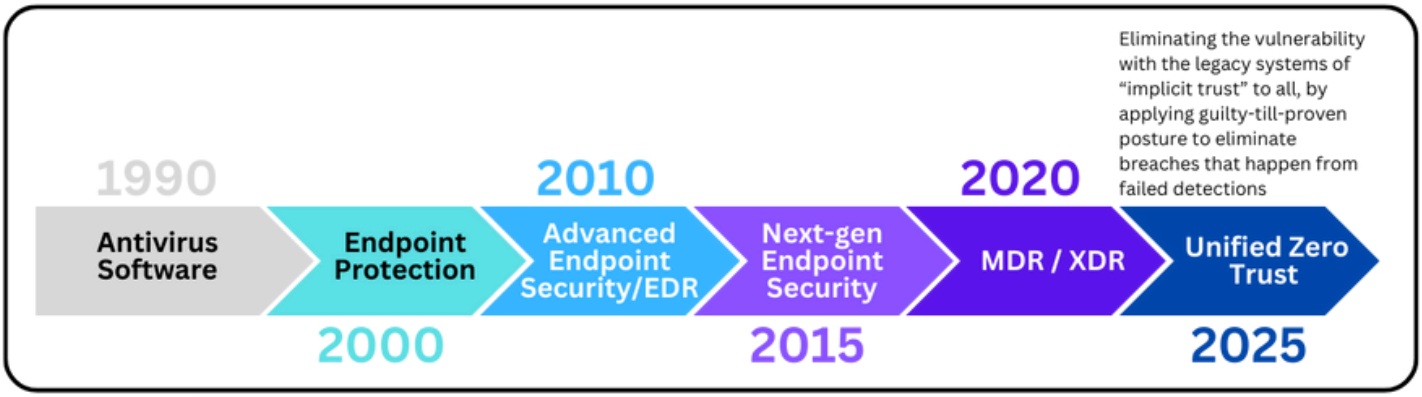
This is where the vast majority of the cybersecurity industry currently sits. At Levels One and Two, protection is excellent – as long as you know what you are looking for. Said another way, If your vendor can detect it they can protect you. But what about the adversaries' innovations that are not detectable because they haven't been seen before? We need a Level Three technology stack that moves beyond partial detection to complete protection.

Level Three - A Unified Zero Trust Platform (UZT)

Since the introduction of EDR there hasn't really been a material innovation changing the code running on endpoints. With UZT the endpoint agent architecture delivers Kernel-level API Virtualization. This overcomes the limitations of Levels 1 and 2 once and for all.

Detection:	All the detection offered by Levels One and Two, but with the important distinction of also being able to detect Known Good and Unknowns. Partial detection (only detecting Known Bad) is overcome with complete protection (also detecting Known Good and Unknown).
Kernel-level API Virtualization:	All Unknowns are identified and addressed with virtualized execution (VX) where they cannot inflict damage, but do not negatively impact the user experience. Unknowns are never assumed safe until proven otherwise.
Verdicting:	With complete visibility into Known Bads (Levels One and Two) and Known Goods (Level Three), Unknowns are easily detected, isolated, and evaluated returning a verdict (either Good or Bad) and addressed accordingly going forward.
Incident Response:	Includes all the incident response capabilities of Levels One and Two, but dramatically reduces the need for IR as nothing slips through the cracks do to faulty assumptions inherent in those levels.
Architecture:	Cloud-native including Level Three Kernel-level API Virtualization

Level 3 - A Unified Zero Trust Platform (UZT)



This three-level technology stack is cumulative not a replacement exercise.

- Of course we need Level One – antivirus
- We must have Level Two – EDR for when antivirus fails
- But protection is insufficient without Level Three – Unified Zero Trust Architecture that removes all blind spots of AV and EDR.

The Unified Zero Trust platform has emerged as the next, and necessary, evolution in cybersecurity. Xcitium's Unified Zero Trust Platform exemplifies this shift, focusing on a holistic security approach that integrates endpoint protection, AV, EDR, XDR, and CNAPP to deliver a Zero Trust cybersecurity posture from endpoints all the way to cloud workloads. Unlike legacy platforms, Zero Trust assumes that no file should be trusted by default. UZT treats every unknown file as untrusted ensuring that no risk is taken with users' security. By overcoming the inherent shortcomings of "assumption-based" cybersecurity, which is all legacy EDR or AV platforms can do, Xcitium's Level Three technology stack has delivered on the promise of true Zero Trust with no assumptions.

Xcitium's Impact: Real-World Results

Device View				
	% of active devices with potential malicious activity (in Containment)	% of active devices on known good state (No Unknowns)	% of active devices that had malicious activity [API Virtualization]	% of Infection/Breach
28 Oct - 03 Nov 2024	13.38%	86.62%	0.4%	0%
21 Oct - 27 Oct 2024	14.23%	85.77%	0.41%	0%
13 Oct - 20 Oct 2024	13.57%	86.43%	0.32%	0%
07 Oct - 13 Oct 2024	11.78%	88.22%	0.32%	0%

Click Here to view most recent results

- **Proactive Protection**: Pre-execution containment stops threats before damage occurs.
- **Zero-Day Defense**: Effectively neutralizes previously unseen threats.
- **Operational Efficiency**: Reduces the need for reactive incident response, saving time and resources.

The Business Case for Xcitium

- **Cost Savings**: Mitigates the financial impact of breaches and reduces response overhead.
- **Regulatory Compliance**: Meets and exceeds global cybersecurity standards.
- **Future-Proofing**: Adapts to evolving threats without the need for frequent updates.

Conclusion: Why Xcitium is the Future of Cybersecurity

Xcitium's Unified Zero Trust Platform sets a new standard in cybersecurity, replacing reactive detection with proactive containment. By eliminating assumptions and delivering comprehensive protection across endpoints and cloud workloads, Xcitium empowers organizations to stay ahead of adversaries and safeguard their digital assets.