Abatis HDF; the case for vendor consolidation in “Endpoint Security”

Abstract:

Platinum High Integrity Technologies does not presume to advise clients on Risk Management in Endpoint Security. Risk Management and therefore risk appetite cannot be outsourced. Our team comprises many I.T security veterans and good practitioners who firmly believe in a multi-layered approach to security and would always advise avoidance of a single point of failure.

However, in recent times to meet ever evolving and increasing threat landscape, often existential, companies and organisations have taken a “belt and braces” approach to I.T security. This has led to a highly complex cyber domain in which multiple security vendors overlap, and has led to an overall unconvincing value proposition with extremely high management overheads, resulting in out-of-control security budgets.

Endpoint Security solutions under review here generally include Anti-Virus, Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) product lines.

The problem in more detail

This is by no means an exhaustive list of the current drawbacks, but rather serves as an indication of how the I.T security protection landscape has evolved with rather negative consequences.

1. I.T Security vendor code is generally resource intensive, invasive & extremely complex.
2. Typical security vendor code over time absolutely and routinely requires emergency security vendor patching as vulnerabilities become known, defined as Common Vulnerabilities and Exposure (CVEs).
3. AV, EDR & XDR companies require a victim to create and deploy mitigation strategies and resolution, which can take days/weeks/months and even years in the case Operating System (OS) vendors. Being reactive in nature the EDR, XDR and AV reactive approach can mean extended intervals of exposure, resulting in intolerable and hard to manage risk.
4. AV, EDR & XDR are considered wide open to unknown malicious code, often described as a zero-day, and an attacker may perform a low and slow (under the radar) co-opting an organisation’s approved toolsets to use against them. E.g., PowerShell, potentially leading to a catastrophic event.
5. Security budgets only go up and cannot be reasonably defined, leading to adversarial conditions with C-Suite.
6. The attack surface is considerably increased due to the sheer size of security vendor code.
7. Having several security overlapping security vendors significantly increases supply chain exposure and act as force multiplier in terms of increased risk.

8. Constant vendor updates introduce risk of "borking" a system or if tested thoroughly in pr-production require a trade off in exposure time yet adding more risk. You are damned if you do and damned if you don't.
9. Multiple security products on an endpoint don't always "play nice" with each other.
10. There is often of a problem of demarcation, a vendor will often deny responsibility for failure to secure. Forensic investigation post a security failure is slow, expensive and doesn't always confirm attribution, nor on many occasions provides for an efficient or capable resolution. Sometimes it can be extremely challenging to absolutely nail down or identify the weakness in a system.
11. Multiple vendors log management can lead to high overheads and storage issues. Often the logs themselves are relatively useless in terms of identifying threat as Advanced Persistent Threat (APT) have readily demonstrated.
12. General Data Protection Regulation can introduce significant financial risk as vendors extract personal identifiable data from your network e.g., reliance on Google's "VirusTotal" service.
13. Vendor management is costly, training, compulsory certification, hosting, travel, eats up I.T management time, leading to huge sunk cost with no business benefit.
14. The conventional reactive model requires that the organisation or business MUST implicitly trust its security provider(s). Often geo-political considerations must be calculated and addressed, especially in the case of National Security or "Cyber Sovereignty". For example, Kaspersky Labs (an AV company with Russian origins) is banned in North America and Huawei have been prevented form deploying their kit in Europe and North America relating to 5G phone networks, ostensibly because for the potential for the Chinese state to gather massive amounts of sensitive data.
15. Who watches the watcher? Your organisation or business is exposed to security providers themselves being hacked. This model can compound insider threat be that malicious, deliberate or even inadvertent, often well outside your sphere of influence. In the last few years notable security vendors of who have introduced malicious code to vast swathes of their global clients include SolarWinds and the then Mandiant's FireEye. (https://www.esecurityplanet.com/threats/fireeye-solarwinds-breaches-implications-protections/)

Platinum High Integrity Technologies proposed solution to the above issues is Abatis HDF.

The Abatis HDF solution can solve most if not all the issues raised above through an entirely different approach to I.T. End Point Security. Prevention – not cure. It is therefore possible by taking the following claims into consideration as a given, to remove multiple layers of redundant security tools and therefore vendors. Platinum High Integrity Technologies would urge a full Strength Weaknesses Opportunities and Threats (SWOT) analysis (https://en.wikipedia.org/wiki/SWOT_analysis) and a full risk appetite assessment before engaging in such an exercise.

1. Abatis HDF is independently (by Lockheed Martin and many others) proven to out-perform all other security vendor I.T Security Endpoint Solutions by preventing any unauthorised code from ingress, be that file-less (living off the land) and/or persistent malicious code including zero-day threat.
2. The Abatis HDF model is based upon Zero-Trust.
3. There has never been a CVE issued against Abatis HDF.
4. The Abatis HDF code has never knowingly been defeated since first deployment in 2005.
5. Abatis protects unsupported legacy estates, some variants of Linux and Microsoft Windows from NT4 to the present Windows 11 & Windows Server 2022, extending asset lifecycle

allowing the organisation or business to upgrade to their schedule, providing controlled investment based upon business need, not an external vendor driven security imperative.

6. For data centre Abatis HDF can provide considerable energy savings.
7. The Abatis software code requires no security updates and does not degrade over time in its effectiveness.
8. The Abatis HDF solution does not require any special Hardware Security Modules (HSM).
9. Abatis HDF is security hardened and self-protecting.
10. Abatis HDF is often used as the last line of defence for high value Network assets.
11. Security Policies can be updated and are fully flexible to meet approved risk appetite.
12. Security Policies can be tailored down to the individual machine or managed in groups of thousands.
13. Abatis HDF is fully scalable.
14. Abatis HDF can be used in Supervisory Control & Data Acquisition (SCADA) and on Programmable Logic Controls (PLCs), in fact wherever there is a resident supported Operating System (OS).
15. Abatis HDF Uses common install tools in deployment and for uninstall.
16. Abatis HDF cannot be removed, nor security policies changed by unauthorised System Administrators as Abatis requires a higher level of privilege, known as an HDF Administrator.
17. The Abatis HDF solution enforces good governance and change control processes.
18. The Abatis HDF does not require any egress of files or any data other than logs in the case of the Managed Security Service Provider (MSSP) model.
19. Each Abatis HDF protected End Point is autonomous, even when disconnected from the Network, making it entirely suitable for air-gapped systems.
20. With Abatis HDF the attack surface is massively reduced, engineers with full physical access to protected endpoint cannot inadvertently infect via USB while undertaking software install or undergoing maintenance.
21. Abatis HDF is relatively tiny – under 40kbs in Windows. The code can be security reviewed under specific conditions, ensuring that there are no back doors.
22. Abatis HDF is deterministic, denies unauthorised code ingress instantly with no human observable latency.
23. Provides empirical logs of actual events with no possibility of false positives or negatives. One deployment model provides for evidential weight standards in logging suitable for the court of law.
24. Works seamlessly with all other security products and tool sets.
25. Abatis HDF provides the ability for patching to your schedule, not just for security tools but ALL software. “Out of band” or emergency patching is no longer required.
26. Depending on the security policy and risk appetite Abatis HDF can render the Operating System (OS) immutable even from forced Original Equipment Manufacturer (OEM) updates.
27. Training is minimal.
28. Operationally this highly capable security solution has the lowest management cost yet known.
29. The solution can be deployed in a few short weeks across multi-national or indeed global networks. Installation on an endpoint takes seconds.
30. Abatis HDF enables I.T security budgets to become quantifiable, known and therefore massively reduce the risk of financial shocks to the organisation or business.
31. Finally, the C-Suite can sleep at night in the sure knowledge that the Abatis HDF I.T security solution simply does what it says it does. PREVENTION not CURE.