SOLUTIONS_

MODERN ENDPOINT SECURITY:

SUPPLY CHAIN SECURITY WITH EDR IS A FORCE MULTIPLIER

INTRODUCTION_

The history of endpoint security has been defined by key moments in which new threats and attacker strategies force security to reinvent itself. The rapid rise of supply chain attacks and vulnerabilities is driving one of those transformations today. These moments do not mean that the old ways are obsolete and should be abandoned, but rather, fundamentally new protections and perspectives are required to deal with fundamentally new threats.

Such jumps in cybersecurity evolution are almost always forced when attackers expose a key assumption or blindspot within the existing security models and products. For example, while antivirus products were the standard of endpoint security for years, attackers learned to subvert their core approach by using rapidly evolving or polymorphic malware, using “living off the land” tactics that reused common IT tools for malicious purposes, and powerful post-exploit kits to disable or evade security controls. The security industry responded with a variety of “detection and response” (EDR/XDR) technologies which focused on looking for malicious or anomalous actions on a host.

However, supply chain attacks have fundamentally changed the landscape once again by shifting the attack to a time and place that defenders logically can’t be, burrowing to places that traditional products can’t see, and most importantly, taking advantage of the implicit trust that most organizations have with their vendors. A supply chain attack doesn’t begin in the enterprise at all, but rather at any of the dozens of suppliers and sub-suppliers of components and code when the product is built. As witnessed during the Solarwinds supply chain compromise, these threats arrive in the guise of valid “trusted” code. Worse still, these threats have introduced new levels of persistence and security evasion, often being buried below the level of the operating system, controlling the boot process of the device, and in many cases, fully subverting or hiding from the OS that EDR products rely on in order to drive detections.

A new generation of Supply Chain Security technologies are addressing this problem and allowing organizations to retake control and proactively verify the integrity of their most critical code, devices, and assets. This approach brings completely new perspectives that knows exactly what code should be on a given asset whether in terms of software, firmware, or physical components. These technologies can verify that all of these elements are authentic, have not been altered, and are behaving appropriately. They go beyond just looking for malicious binaries or actions, and additionally audit how all the components and available protections work together as a whole device or system. So instead of ceding the advantage to attackers and forcing defenders to reactively detect and respond, organizations can now proactively and continuously verify that the critical code on their devices is actually worthy of trust. And instead of replacing EDR, these new capabilities vastly enhance these products to give organizations the best of both worlds.

HOW SUPPLY CHAIN SECURITY (SCS) AND EDR FIT TOGETHER_

Supply Chain Security and EDR can work together and complement each other quite well. Naturally, there is some overlap between the technologies – they both are able to detect threats and vulnerabilities, for example. But some level of overlap between security tools is a good thing. You get a level of defense in depth by being able to detect threats from multiple perspectives. However, for the most part, Supply Chain Security and EDR take very different approaches, and these differences allow Supply Chain Security products to do things that no other class of security does today. Let's take a look at some specific examples.

Integrity Verification

Supply Chain Security tools bring a completely new perspective to security that proactively verifies the integrity of a device, and all of its critical components and code. This ability to "verify the good" instead of just "detecting the bad" requires a completely different set of capabilities. For example, it requires the solution provider to maintain a massive and constantly changing database of all the valid critical code within an endpoint. For example, Eclypsium monitors more than 6 million elements from over 200,000 update packages, covering more than 95,000 distinct devices that include a vast range of vendors, device types, and models. This database is an absolute requirement in order to verify that attackers have not tampered with or altered the underlying components of a device in the supply chain.

This allows organizations to find problems before a new device or update ever runs, instead of having to wait and hopefully detect malicious actions after they've run. It shifts security far earlier in the technology lifecycle and makes security far more proactive. This directly compliments an EDR. Instead of an EDR having to play catchup by detecting a threat, organizations can verify they are starting from a good place and then rely on EDR to detect new threats coming from the outside.

Device and Component Expertise

EDR tools focus on the actions happening on a device, whereas Supply Chain Security audits the device itself. The average endpoint has 15-20 different critical components that run their own pre-installed forms of software and firmware, and servers can have 30 or more. This can include:

1. **Unified Extensible Firmware Interface (UEFI or EFI):** Typically the most privileged and critical code on a device. Malicious firmware implants can give attackers complete control over a device
2. **Bootloaders:** Governs how a device boots, with vulnerable bootloaders allowing an attacker to gain full control over a system.
3. **OS Device Drivers:** Extend the OS kernel with OEM hardware specific capabilities. Vulnerable drivers have regularly been used by APTs (e.g. LoJax) and ransomware groups (e.g. Lazarus)

4. **Baseboard Management Controllers (BMCs):** Provide out-of-band management for servers. Have been targeted by attackers to take full control of servers and even entire data centers (e.g. iLOBleed)
5. **Trusted Platform Module (TPM):** A dedicated hardware chip critical for establishing root of trust and strengthening full-disk encryption. Vulnerabilities put these critical capabilities at risk.
6. **Chipset Components:** Example include Intel Converged Security and Management Engine (CSME aka ME), Active Management Technology (AMT) and AMD Platform Security Processor (PSP)
7. **System Management Mode (SMM) Firmware:** This is the runtime firmware that governs the low-level components of a device. Attackers have used this to control a device while remaining completely invisible to the OS.
8. **Network Controllers:** Can include wired NICs, WiFi adapters, Cellular, Bluetooth, etc. These controllers are completely invisible to modern endpoint security measures, yet have large remotely exploitable attack surfaces.
9. **Hard Drives and SSDs:** Highly targeted APTs (e.g. GreyFish and Equation Drug) have compromised these components as a way to hide malicious code in segments of drives that can remain hidden from the OS.
10. **CPUs:** Low-level issues in CPU firmware and microcode have resulted in serious issues such as Spectre, Meltdown, Portsmash, Foreshadow, MDS and others.

These are just ten of the most common examples. All told, these and other components can constitute hundreds of thousands executable modules and millions of lines of code developed by manufacturers and hundreds of hardware and software suppliers, each of which is a potential target of a supply chain attack. A Supply Chain Security solution specializes in these components, which remain largely outside the purview of EDR tools. The combination ensures organizations can audit the device itself as well as what happens on the device in higher layers.

OS INDEPENDENT AUDITING_

EPP and EDR tools were designed to work “from the OS and up to applications.” This design also means that they are heavily reliant on the OS for the information that they use to detect threats. Supply chain attacks can compromise a wide range of code that can sit below the operating system. This has allowed attackers to run malicious code that can either manipulate the OS to remain invisible or report false information. For example, UEFI implants or malicious bootloaders can allow attackers to patch the OS at boot time. Threats like iLOBleed have used compromised firmware to report false information, and SMM attacks can halt the OS to execute malicious actions that are invisible to the OS. This is not only a security blindspot, it also creates a circular problem where higher layer security tools can’t truly trust the information they are seeing from the OS.

Supply Chain Security solutions specialize in these areas and will collect low-level data in multiple ways including methods that are independent of the operating system. They likewise include specialized drivers needed in order to reliably see and analyze critical code in software and within components. This deep visibility also allows SCS tools to reliably analyze the low-level behavior of critical code and components to identify threats that may have been introduced in a vendor’s valid, signed code as was the case in the SolarWinds attack. By combining SCS and EDR, organizations can maintain comprehensive visibility across a device, while ensuring that the data they see in their EDR can be trusted.

KNOWING HOW IT ALL FITS TOGETHER_

At the end of the day, EPP and EDR tools are looking for malicious code. They have many ways of doing this, but their scope is ultimately at the level of a "threat". Supply Chain Security adds a true system-level perspective. Each end-point is a complex amalgamation of systems and components from dozens of suppliers, sub-suppliers, OS vendors, chipset vendors, OEMs, and so on. While each of these components must be audited individually, it is just as important to make sure that it is all working together properly.

For example, a modern "Secured-core" PC requires OEMs to bring together a variety of protections from different vendors and configure them in a very specific way. If a single bit gets flipped or the right setting isn't enabled, then the collective protections can fall apart. There is a very long history of this happening. Again, traditional tools have limited scope in that they focus on specific exploits, malicious binaries, or vulnerabilities whereas Eclypsium validates the product or service as a whole.

APPLYING UPDATES_

In addition to detecting and responding to threats, Supply Chain Security products help organizations to remediate the flaws and vulnerabilities in their infrastructure. Once again, supply chain tools focus on remediating problems in low-level settings, configurations, and code that are often below the level seen by traditional software vulnerability scans. Furthermore, the unique domain expertise found in supply chain security tools can helps prioritize and actually address the most critical issues. In short, these tools can help teams answer the questions "Should I update" and "How do I update"? These capabilities allow security teams to:

- Proactively fortify their devices to reduce the overall attack surface of the organization.
- Provide automated scheduling, staging and deploying most appropriate to the device.
- Deploy critical updates across all major devices in the endpoint fleet.

CONCLUSIONS_

The rise of supply chain attacks allows threat actors to exploit the trust organizations have with their technology suppliers. In order to address these risks, organizations need security tools that understand supply chains and their unique vulnerabilities and threats. EDR and Supply Chain Security share some high-level similarities in that they both focus on security at the device level. However, they actually work quite differently and address different problems. Supply Chain Security brings the deep industry-wide understanding of supply chains that is required in order to proactively and independently verify the integrity of an organization's assets, find vulnerabilities and threats, and take the appropriate actions needed to mitigate the risk.

ABOUT ECLYPSIUM_

Eclypsium is a supply chain security platform for modern endpoints, servers, network devices, that enables organizations to build trust in every device by identifying, verifying and fortifying software, firmware and hardware throughout enterprise infrastructure, including all third-party components. Eclypsium's SaaS platform provides comprehensive visibility into every device, discovers vulnerabilities, ensures integrity, and enables management of critical updates across entire device fleets.