The Long-Term Evolution of Endpoints Will Reshape Enterprise Security

Published 1 May 2019 - ID G00365511 - 13 min read

By Analysts Dionisio Zumerle

Endpoints are becoming digital consumer experience enablers that are more tightly controlled and natively fortified against attacks. Security and risk management leaders must design long-term security and investment strategies that align with this technology trend.

Overview

Impacts

- Providers of operating systems for user endpoints will increase the fortification of these endpoints, which means both attackers and enterprises will see their options for control drastically reduce, having to resort to alternative ways to protect endpoints.
- Endpoints become vessels for digital consumer experiences, interfering with enterprise workflows and causing exceptions, noncompliances and security gaps, while their transformation shifts attacker focus to the authentication and authorization domain.

Recommendations

Security and risk management leaders responsible for endpoint security should:

- Increase focus on endpoint security hygiene as endpoints become natively hardened and enterprise control decreases. In particular, structure your device vulnerability management and application vetting capabilities.
- Leverage synergies with native OS capabilities and adjacent tools. As platform lockdown decreases visibility into the endpoints, correlation of information from multiple data sources other than endpoint security will be fundamental.
- Replace endpoint micromanagement with software-defined perimeters focusing on the application layer. Allow endpoints access to information on a need-to-know basis, adapted to the level of assurance that these endpoints can provide.

- Navigate the “consumer wave” to ensure user enablement and compliance. Where endpoint ecosystems and BYO break workflows, use a three-level strategy that includes defining acceptable usage, enabling security measures on top, and imposing sanctioned alternatives.

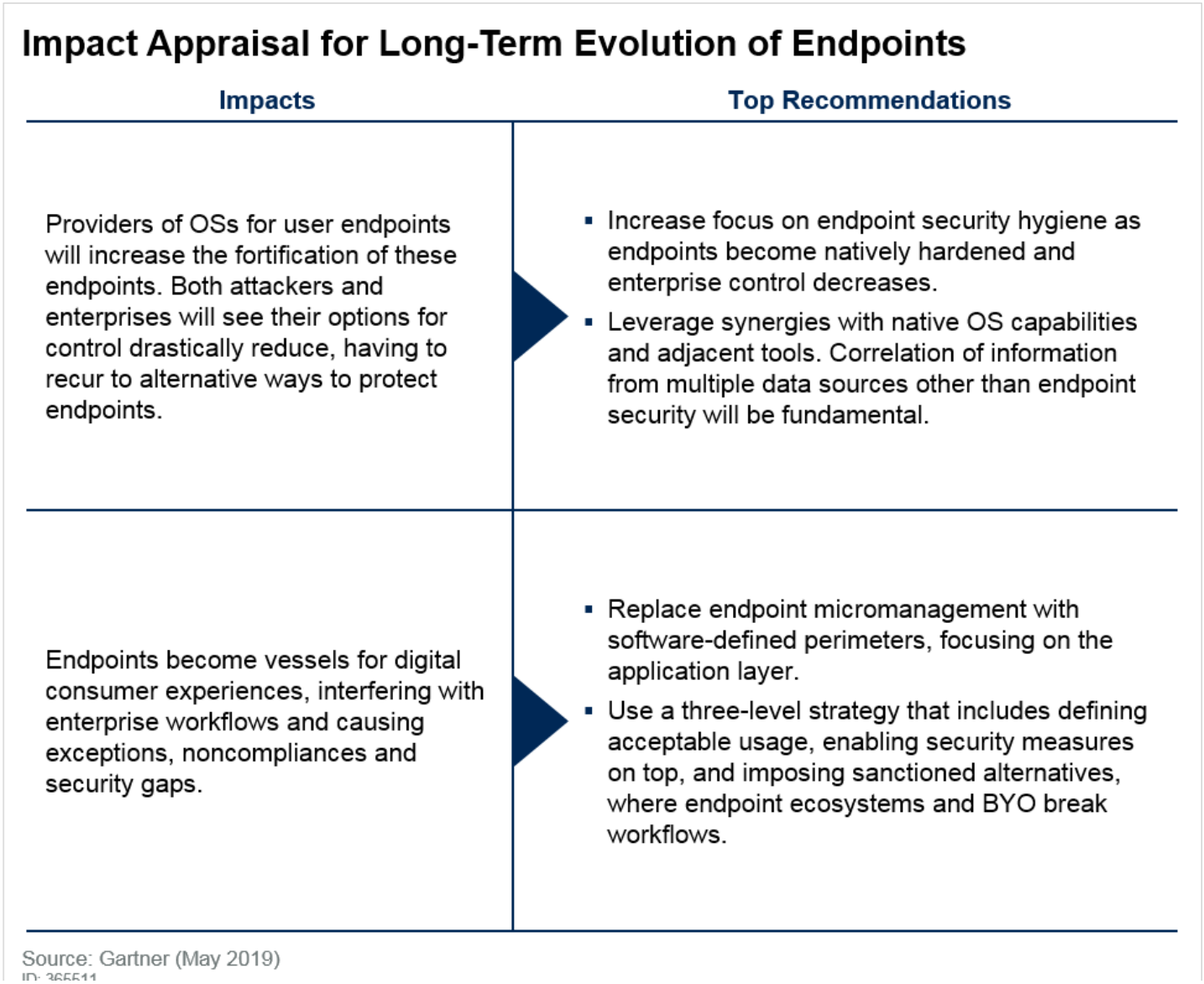
Strategic Planning Assumption

By 2025, more than 85% of successful attacks against modern enterprise user endpoints will exploit configuration and user errors, rather than make use of advanced malware.

Analysis

The providers of user endpoint OSs and platforms, namely Apple, Microsoft and Google, are transforming their offerings. Long-term enterprise security strategies will have to adapt by shifting the focus of endpoint security controls to domains other than traditional anti-malware technology.

Figure 1. Impacts and Top Recommendations for Long-Term Evolution of Endpoints



Impacts and Recommendations

Natively Fortified Platforms Reduce Risk and Visibility

Endpoints become more controlled and locked down by technology providers, reducing risks but also reducing security tool visibility and control. Endpoint operating systems are increasing their security controls in three main ways (see Figure 2):

- **Platform hardening.** Unlike traditional personal computer endpoints, mobile devices have always been locked down. For example, a user of an iPhone or an Android device does not have administrative privileges over the platform. This built-in hardening has kept mobile security incidents to a minimum thus far, while attacks against PCs have been growing. [1] [2] [3]

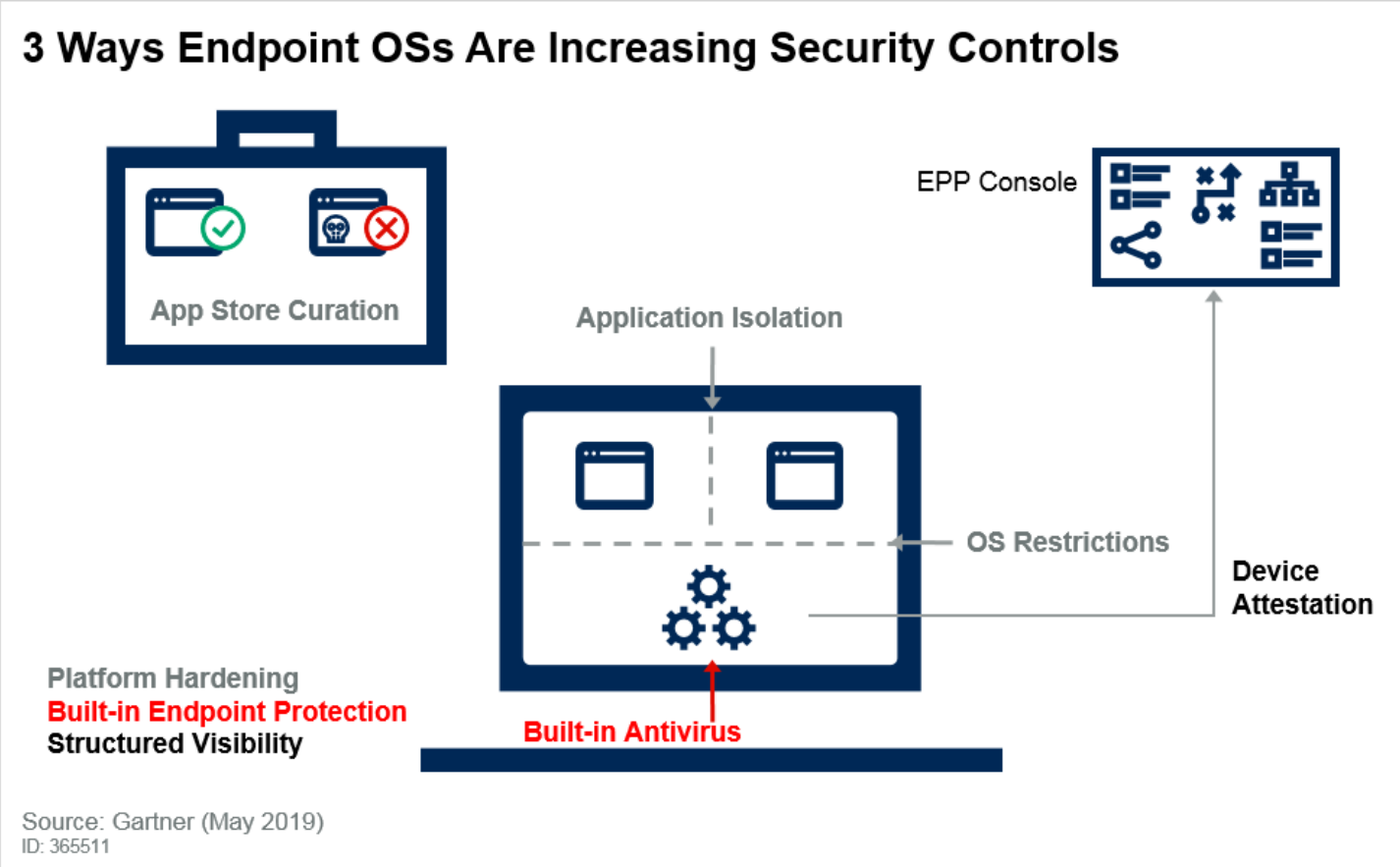
  There are indications that Microsoft is following the footsteps of mobile platform providers in hardening the Windows 10 platform [4] and removing harmful applications. [5] Some of the traits of platform hardening are:

  - Hardware-based root of trust
  - Automated updates
  - Restriction of OS and kernel-level calls from applications
  - Application isolation from each other
  - Application vetting via an application store (see "Windows 10 Enhances Security")

- **Built-in endpoint protection.** With varying degrees of maturity, all modern endpoints already provide native active protection mechanisms, in addition to hardening. Examples of this are the macOS Gatekeeper, Windows Defender and Android's Google Play Protect. Endpoint providers will work on and strengthen these mechanisms.

- **Structured visibility.** We expect endpoints to also provide more controlled ways to obtain visibility into the endpoint. For example, instead of freely accessing the kernel space, a security tool or application can invoke the SafetyNet Attestation API [6] to verify a device is in a trusted state. It can also leverage the NetworkExtenstions API in iOS to obtain visibility onto a device's network traffic without proxying any of the traffic. [7]

Figure 2. Three Ways Endpoint OSs Are Increasing Security Controls



As a platform, Windows 10 must prioritize that the myriad legacy applications that run on PCs today remain operational. A hard transition today would create incompatibility issues for many, if not most, organizations. Therefore, a complete transition to a fully locked-down platform will not happen before 2025. Security and risk management leaders need to begin aligning their long-term strategies with this trend now.

Once complete, platform hardening will decrease the success rate of traditional attacks against endpoints. At the same time, it will reduce the extent of the freedom that endpoint protection platforms (possibly along with nonsecurity tools) have over endpoints. It will also favor products that more actively leverage native protection features.

Recommendations:

- **Increase focus on endpoint security hygiene.** Newer endpoints will have more restrictions on code execution, which makes it more difficult for attackers to run malicious code and for malicious code to cross application boundaries. However, malware countering is only part of endpoint security duties. With endpoints hardening, application delivery will be performed via app store distribution mechanisms of signed applications. This will decrease the need for additional malware countering as these stores foresee a scanning for these applications. However, it will do so only as long as endpoints adhere to a predefined security baseline. They must:

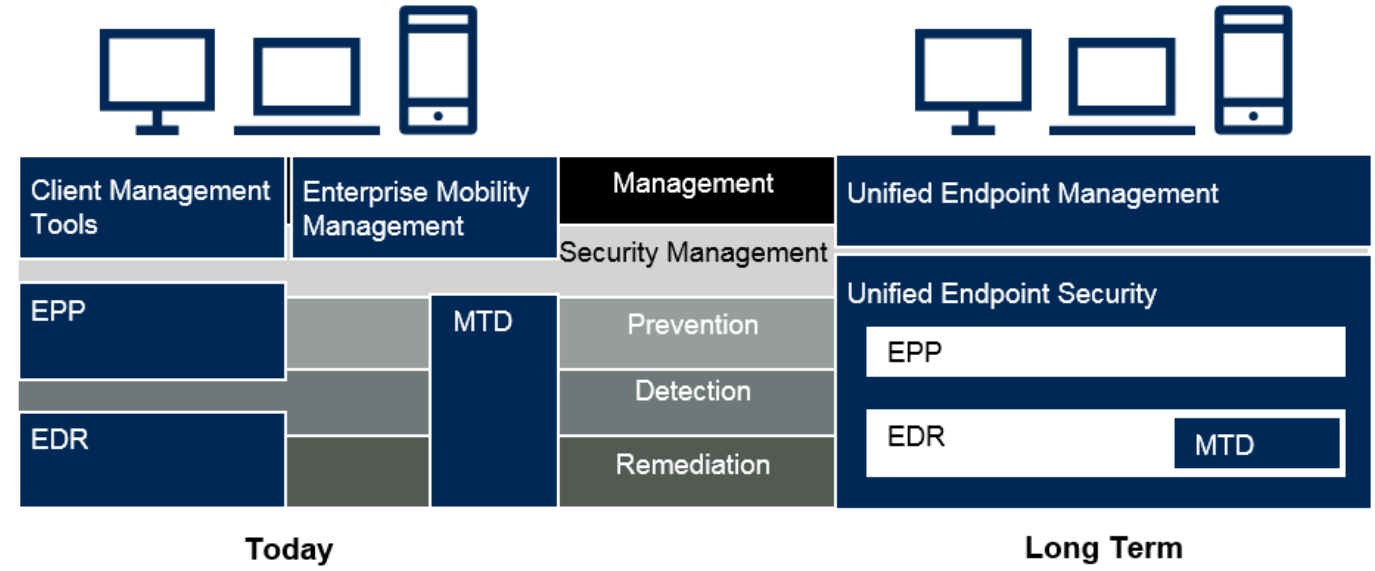
- Provide structured device vulnerability management. Security leaders will have to strengthen their processes for endpoint discovery, inventory and vulnerability assessment. From a tool standpoint, focus on endpoint security products that can assess endpoints, identify missing patches and take actions to bring the endpoints back to compliance. Examples of such tools that today have support for Windows 10 are 1E's Tachyon, Ivanti's Endpoint Security for Endpoint Manager, Promisec and Tanium. In this endeavor, further interaction with unified endpoint management (UEM)/client management tool (CMT) and IT asset management (ITAM) tools can help (see the following bullet as well as "Building the Foundations for Effective Security Hygiene").

- Focus on application vetting as part of application control. Assuming the native controls greatly reduce the presence of malware, enterprise focus should turn to application vetting. This is a variation of application control (see "How to Successfully Deploy Application Control") that is not focused on lockdown, but on identifying and removing grayware. Grayware indicates applications that are in conflict with enterprise policies. An example can be an application that exfiltrates enterprise contact details to an advertiser.Many endpoint protection platform (EPP) vendors today provide application allow-listing and block-listing mechanisms. In the future, we expect a more granular approach (mobile threat defense [MTD] vendors already provide this for iOS and Android), allowing the enterprise to define acceptable behavior of an application, and automatically impose this policy through an application scanning tool. Part of this exercise would also require enterprises to sign all the applications they produce and have an application-signing governance process in place.

- **Leverage synergies with native capabilities and adjacent tools.** Among the effects of the evolution of endpoints will be that attacks will try and bypass the new hardening mechanisms. Detection (via solutions such as endpoint detection and response [EDR]) is fundamental to stop attacks that bypass these built-in defenses. However, this same native hardening that is fortifying endpoints is also decreasing the visibility and system privileges that security tools need in order to detect and remediate attacks. As platforms evolve, endpoint security will need to implement mechanisms to compensate for this loss, such as:

  - Integrating endpoint security tools with endpoint management tools. Actions such as device discovery and device vulnerability management are closely linked to client management and UEM tools. During the detection phase, management tools can provide useful information (such as the application inventory of a device) to security tools. Among other things, they leverage structured visibility to do so. During the response phase, the security tool identifies a threat, asking the UEM tool to take a remediatory action. The present and future relationship between endpoint management and security tools is illustrated in Figure 3. (See "When and How to Go Beyond EMM to Ensure Secure Enterprise Mobility" for an example of how these synergies already take place between UEM and MTD tools.)

Figure 3. Present and Future of Endpoint Management and Security



Source: Gartner (May 2019)
ID: 365511

As visibility and privileges on the endpoint decrease, management tools will remain privileged entities on the device. Enterprises with good integration between these management tools and security tools will be able to provide their security teams with the necessary information to detect and investigate incidents and to coordinate hardening and remediation with operations.

- Leveraging endpoint security tool synergies with network security. "How to Decide Whether Endpoint and Network Security Integration Is a Feature or a Fad" analyzes how correlation between network security and endpoint security events can improve visibility and detection rates of attacks. Going forward it will be increasingly important to compensate for loss of deep visibility into the endpoint and, to be able to correlate not only network security activity, but any connected activity. Hence, integration with cloud access security brokers (CASBs), secure web gateways (SWGs), next-generation firewalls (NGFWs) and EPP suites will be fundamental.

Endpoints Become Hosts of Digital Consumer Experiences, Interfering With Enterprise Workflows and Causing Exceptions

Endpoints are not locking down for security reasons exclusively. The device market is turning its focus to enabling vertical digital ecosystems and experiences. [8] , [9] These are designed to revolve around the usage of virtual private assistants and interactions with cloud-based vertical ecosystems. In the future, they will involve the usage of connected endpoint devices (such as, car entertainment, TV and smartwatches) that blur digital interactions with physical experiences. [10] As part of this transformation, newer operating systems are introducing a fundamental shift in endpoint data

storage from a default local storage to a default distributed cloud strategy. This change will shift attacker focus to the authentication and authorization domain. [11]

With the increase in endpoint fortification, enterprises will no longer be able to apply the same enterprise control and fine-tuned device security management as before. Additionally, as these digital interactions intertwine with enterprise workflows, they create noncompliances and security gaps, as they do not fully align with these ecosystems.

For instance, consider employees using Siri to send an iMessage through their MacBooks. In a regulated environment, such as the financial one, this message would have to be archived; but the Apple ecosystem has restrictions on iMessages that do not allow for seamless archiving (similar issues would apply with WhatsApp). (See "Market Guide for Instant Communications Security and Compliance" for more details.)

Compounding these concerns are the data gathering practices and privacy policies that many of the consumer applications and ecosystems present.

The inexorable increase in bring your own (BYO), which is touching mobile and other connected devices, wearables and PCs as well as IT itself, [12] , [13] exacerbates this issue. Indeed, the more personal devices enter the workplace, the more challenging it will be to single out the consumer experience platforms the devices run on, and the data that is collected while enabling these experiences.

Recommendations:

- **Replace endpoint micromanagement with a software-defined perimeter (SDP).** As platforms gain stricter control over the device, enterprise lockdown of the device will need to decrease. Indeed, with BYO growing and with modern endpoint interactions consisting of personally owned devices interacting with third-party clouds, less and less granular and customized management will be feasible on the device. To compensate, the focus will move from devices to applications, where the organization can gain back some of the lost control and granularity. There will be a shift from statically imposing strict policies on devices to dynamically deciding whether to allow a specific action that involves access to enterprise resources. This decision will be based on whether the device satisfies certain security criteria, or whether its "risk score" is under a certain threshold. The term software-defined perimeter, zero-trust network access, is often used to refer to this concept (see "Zero Trust Is an Initial Step on the Roadmap to CARTA" and "Market Guide for Zero Trust Network Access"). The broader concept of dynamic access based on satisfying of certain conditions is also usual in consumer-facing scenarios, and is often put in place via online fraud detection tools; but its application to enterprise devices is still emerging (see Figure 4).

Figure 4. Endpoint Security's Role in Zero-Trust Architecture

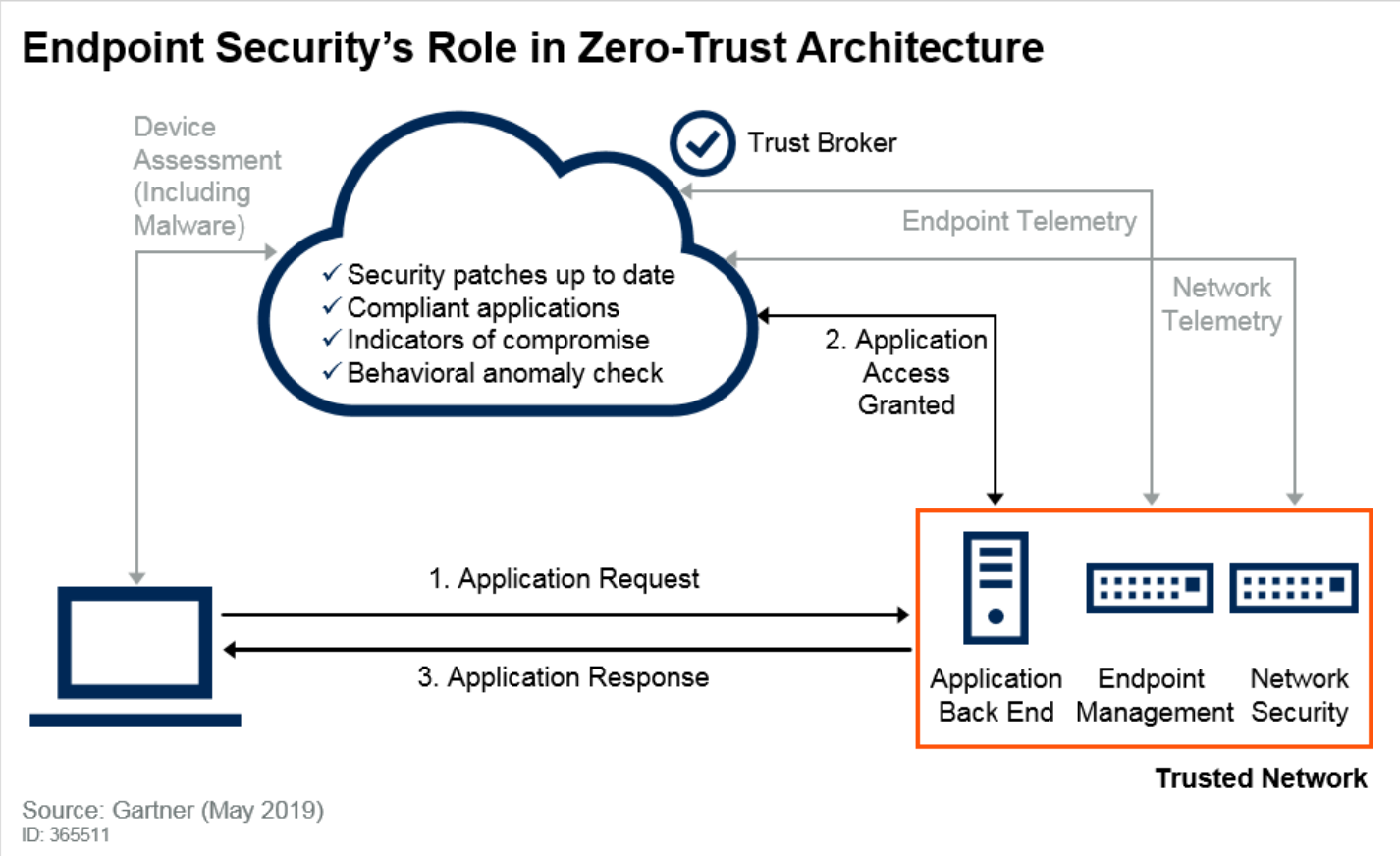


Figure 4 illustrates a model of this mechanism. In addition to stand-alone SDP vendors, network access control (NAC), SWG, CASB, identity management [IdM], MTD and EPP vendors are delivering relevant functionality. An example of this mechanism today is Microsoft's Azure Active Directory (Azure AD) conditional access. [14] Also related to SDP is the concept of adaptive access control (see "Evaluation Criteria for Access Management"). There are three main logical components (these can be aggregated or decoupled depending on the solution) that are central to an endpoint-focused SDP:

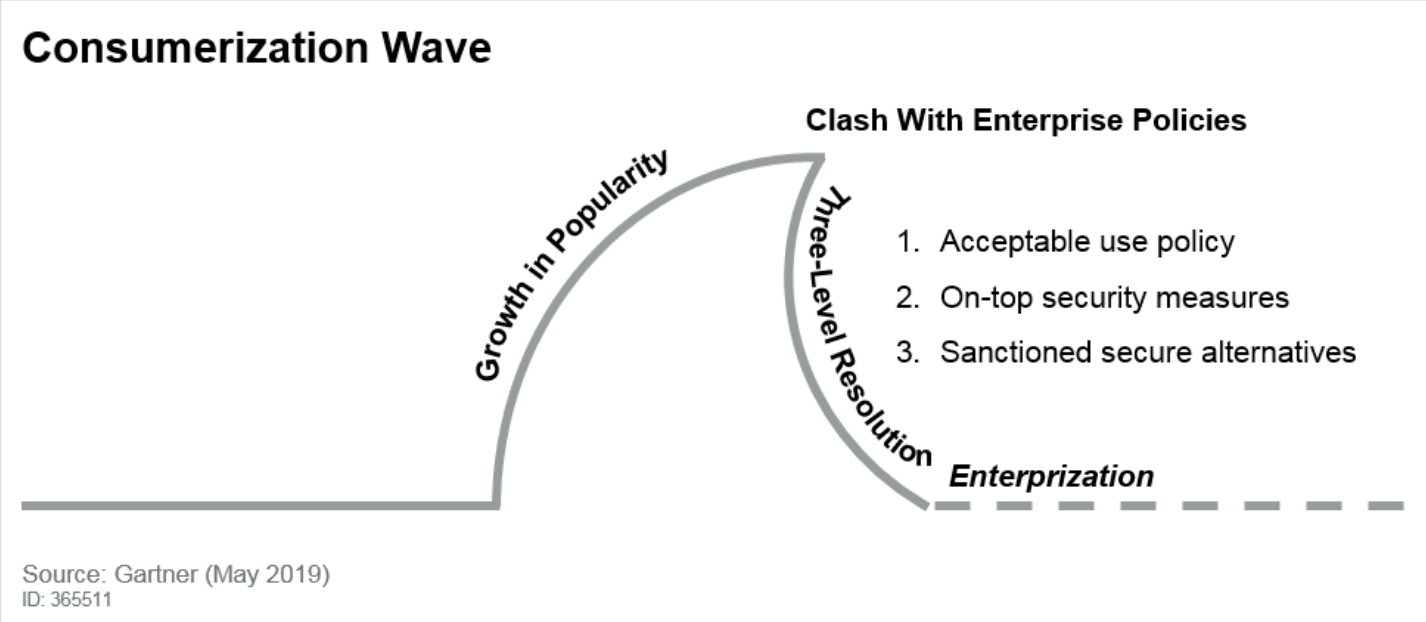
- An identity component — This component is in charge of determining the identity of the user or entity that requests access. It can include a behavior-based component and protection specialized against account takeover, such as multifactor authentication.
- A device assessment component — This component is specific to endpoint security scenarios and assesses the level of trust that can be placed on the device. The assessment will include checks for malware, whether the latest patches are deployed, whether the device is corporate or personal, and others.
- An access component — This component will include transport security. Beyond a simple secured tunnel or an authorization software, there can be innovations in this space. For example, MTD solutions from Lookout and Symantec provide blackholing, that is, a mechanism

that can block devices from accessing enterprise resources when they demonstrate suspicious behavior. [15] , [16]

SDP projects are already becoming popular, but not every organization will be ready or fit to adopt this concept. "Fact or Fiction: Are Software-Defined Perimeters Really the Next-Generation VPNs?" provides an analysis of use cases that may fit the SDP model.

- **Navigate the "consumerization wave" to ensure user enablement and compliance.** The consumerization wave (see Figure 5) foresees a phase where an ecosystem or application meets growing popularity. This popularity makes it more and more present in employees' lives, to the point that it starts mixing and impacting work, and clashing with enterprise policies by the time it reaches the crest of the wave.

Figure 5. Addressing/Navigating the Consumerization Wave



In rare instances, the ecosystem or application develops an enterprise version or enterprise capabilities that resolve the conflicts with enterprise policies. Most often, however, enterprises are not that fortunate, and at the crest of the wave they must take action to resolve the conflicts. A three-level strategy can help in this process.

1. An enterprise devises a policy.
2. On-top security measures are added to mitigate risks.
3. Stand-alone measures are added to provide equivalent enterprise experiences. [17]

Applying this concept to the iMessage example presented earlier, the first level would mean adding a section on messaging and social media in the mobile policy. As part of this step there should be an evaluation of the regulatory and legal impact of transit and storage of sensitive data in the cloud. The second level would perhaps require adding a data loss prevention (DLP) solution to prevent sensitive documents from being sent via iMessage. Finally, the third level could mean implementing a stand-alone instant communications solution that replaces iMessage. (See "Take These Four Steps to Securely Use WhatsApp, WeChat and Other Instant Communication Apps" for further details on this use case.)

As new applications become popular and platform ecosystems evolve, this will be an ongoing exercise against a moving target, which will require periodic refreshes.

Evidence

[1] "Verizon Data Breach Investigations Report (DBIR)." Verizon.

[2] "As Phones Get Harder to Hack, Zero Day Vendors Hunt for Router Exploits." Motherboard.

[3] "Research Firm Offers $3 Million for iOS, Android 0-Days." SecurityWeek.

[4] "Windows 10 S Security Features and Requirements for OEMs." Microsoft.

[5] "Windows 10 Fall Creators Update: syskey.exe Support Dropped." Ghacks.

[6] "SafetyNet Attestation API." Android Developers.

[7] "NetworkExtension." Apple Developer.

[8] "Seize Consumer Opportunities for PCs, Smartphones, VPA Speakers and Connected Home Devices in 2018."

[9] "Millennials: Attitudes Toward AI and Personal Devices."

[10] "Predicts 2018: Personal Devices."

[11] "chrome.storage." Chrome Developer.

[12] "How CIOs Should Prepare for the Risks From the Next Wave of BYO."

[13] "Citizen Development Is Fundamental to Digital Transformation."

[14] "How To: Require Managed Devices for Cloud App Access With Conditional Access." Microsoft Azure.

[15] "Lookout — Post-Perimeter Security." YouTube.

[16] "SEP Mobile — Selective Resources Protection Overview." Symantec Support.

[17] "Market Insight: Enabling Smart Workspaces to Support Future Digital Business — Devices' Role."