IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Illumio

Preventing threat actors from moving from one infected endpoint to another is essential in today's disaggregated digital footprint. Visibility and allow-list policy controls make this possible without interfering with legitimate business operations.

Curb Malware Spread with Comprehensive Visibility and Allow-List Policy Control

July 2021

Written by: Michael Suby, Research Vice President, Security and Trust

Introduction

End-user devices are frequently the initial point of compromise in cyberattacks. From the first infection, threat actors move laterally to other systems, spreading malware, gathering credentials, conducting reconnaissance, and creating back doors to exploit higher-value assets (i.e., servers and workloads) or, in the case of ransomware attacks, threaten to disrupt critical business operations.

While endpoint security solutions have been effective in preventing a widening array of attacks at first encounter, advanced malware and ransomware continue to bypass these solutions and wreak havoc on organizations. Endpoint detection and response (EDR) adds another layer of much-needed defense, but even the combination of protection and EDR is insufficient. The potential for a security breach is reduced but not eliminated.

AT A GLANCE

KEY TAKEAWAYS

- Current approaches to cybersecurity leave too many communication channels open for threat actors to succeed in nefarious objectives as evidenced by massive malware infections and ransomware attacks.
- Organizations can fight back with an allow-list approach built on comprehensive and authentic visibility of traffic flows among endpoints and applications. With this approach, traffic flows are restricted to only those that are necessary for the business. The rest are automatically blocked.

In light of an inevitable infection, organizations must do better at containing threats and restricting threat actors' range of movement. Ultimately, the goal is to make the first infection the last infection. Legacy approaches, such as host firewalls, group policy objects (GPOs), and network access control (NAC), exist to support this objective, but limitations, complexity, and cost have hampered their use and effectiveness. Another approach, closing down the communication conduits used by threat actors to move from one system to another, is purpose built to prevent threats from spreading.

Consider the many peer-to-peer communication protocols that exist to support specific use cases (e.g., RDP, SMB, FTP, NFS, and WMI) — and are also channels for malware propagation that can quickly evolve to mass infections. While they exist, not all of them are needed for all systems. Allowing communication between systems over protocols that are not routinely needed, in essence, provides an unrestricted conduit for threat actors to move from one system to another. Conversely, allowing communication only over essential ports and protocols and disallowing the rest is an effective countermeasure and aligns with the principle of zero trust.

But what appears to be effective can become ineffective if the means to create and enforce allow-list policies is complex and cumbersome. This IDC Technology Spotlight describes an allow-list approach that is simple to use and extensible to controlling application access.

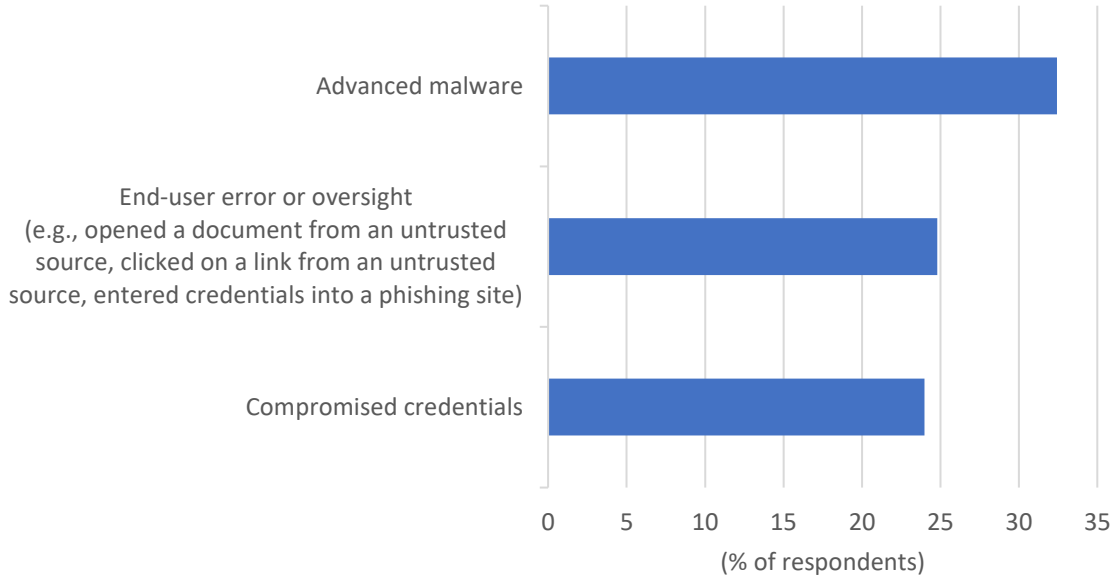
Endpoint Security Risk Continues to Rise

The digital footprint of today's organizations is an open and evolving mass of connections among distributed systems — end-user devices, servers, workloads, and SaaS applications. Unfortunately, the system-to-system connectiveness that powers organizations is also the highway for threat actors to transmit their malicious payloads quickly and broadly from one system to another. The consequences can be severe. According to an IDC survey of security professionals, advanced malware is the most frequent contributor to security breaches (see Figure 1).

FIGURE 1: ***Most Frequent Contributors to Security Breaches***

Malware, end-user error or oversight, and compromised credentials are the top 3 most frequent contributors.

Q ***Which of the following are the most frequent contributors to security breaches? Please select up to 3 contributors from the list of 13.***



n = 367

Source: IDC's EDR and XDR Survey, December 2020

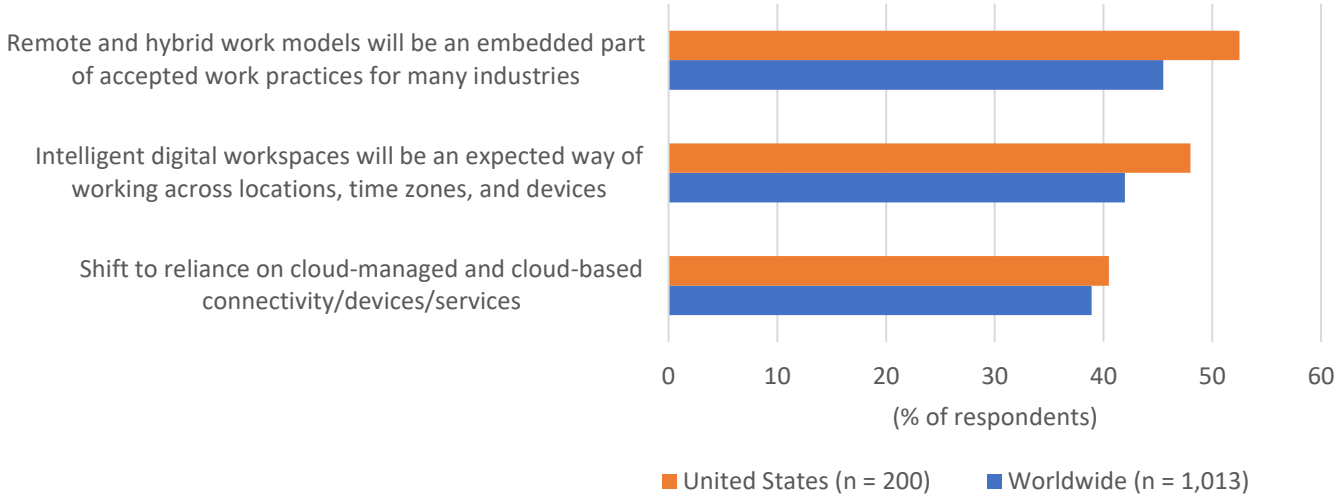
Another noteworthy finding from the survey is that end users frequently open the door to let threat actors in. This situation, unfortunately, worsened with the pandemic as employees were cast into remote working arrangements, confronted with new workday distractions, anxious to stay informed on current events and, quite possibly, less diligent in their security practices. Knowing an exploitable situation when they see one, threat actors pounced. In 2020, the number of pandemic-themed phishing sites and emails soared and RDP grew as a popular means for ransomware delivery. These circumstances are unlikely to change. According to an IDC survey conducted in February 2021, remote and hybrid work

arrangements will persist for many organizations (see Figure 2). IDC has no doubts that threat actors will continue to exploit this situation, using pandemic-themed enticements in fraudulent websites and email subjects until another topic grips people's attention.

FIGURE 2: ***Top 3 Post-Pandemic Enduring Work Practices and Technologies***

Remote and hybrid work models top the list.

Q ***In your opinion, which work practices and technology advances emerging from the pandemic are most likely to endure?***



Source: IDC's Future Enterprise Resiliency and Spending Survey, February 2021

As organizations have become increasingly digitally interconnected, the implications of endpoint infections and malware spread have grown. Furthermore, financially motivated threat actors are quick to branch out from the first compromised endpoint to reach additional systems and corporate applications.

While most organizations have equipped themselves with endpoint protection platforms (EPPs) and EDR to mitigate cyber-risk, there are no guarantees that malware will be contained before critical business operations are disrupted, employee productivity is interrupted, and sensitive data is exfiltrated. As evidence, global corporate insurance carrier Allianz reports in *Managing the Impact of Increasing Interconnectivity: Trends in Cyber Risk* (October 2020) that cyber-related insurance claims have been on a steady upward trajectory since 2015. In 2020, malware and ransomware incidents increased by more than one-third.

With infections inevitable, organizations must consider their options to further reduce the risk of malware spread and broadly penetrating ransomware attacks. An allow-list approach that reduces system-to-system traffic flows to only those that are explicitly permitted is a promising technology that augments the preventive capabilities of EPP and the post-infection containment of EDR.

A Five-Step Approach to Enforcing Allow-List Policies

An allow-list approach restricts endpoint-to-endpoint, endpoint-to-server, and endpoint-to-application traffic flows to only those an organization explicitly defines as legitimate. Only trusted traffic flows that serve business objectives are allowed. All other flows are automatically blocked. For organizations striving to incorporate zero trust and micro-segmentation into their security architectures, an allow-list approach is tightly aligned with those efforts. Traffic to business applications (licensed, custom, and SaaS) is controlled through defined segments of allowed endpoints, applications, and context (e.g., on network versus off network).

Five Steps to Enforcing Allow-List Policies for Zero Trust Endpoint Protection

Step 1: Visualize traffic flows. Essential in the creation of effective allow-list policies is a centralized and detailed visualization of traffic flows between endpoints and with applications. While visualization is at the network level (i.e., every port and protocol), visualization cannot solely be from endpoints that are on the network. With remote working and expanding use of SaaS, traffic flows must be collected from endpoints regardless of location — on and off the network. Visualization based on traffic flows from a 30-day period or longer improves the quality of allow-list policies, resulting in reduced false positives (i.e., blocking legitimate traffic) and false negatives (i.e., allowing illegitimate traffic).

Operationally, visualization in a cloud-based platform is preferred. There is no new infrastructure to deploy, configure, and manage, and the rapid scalability necessary to collect and visualize traffic flows from all endpoints is innately supported. In addition, direct collection from remote endpoints is more resource efficient than forcing collection through a centralized on-network server.

Step 2: Group endpoints. Although an allow-list approach theoretically can support a unique set of policies for each endpoint, grouping "like" endpoints is more realistic. In practice, policy administrators will examine endpoints' historical traffic flows along several dimensions. Potential dimensions include:

- End-user affiliations (e.g., department, role, and title)
- Device type (laptop versus smartphone)
- Operating hours (work hours versus non-work hours)
- Location (onsite versus remote)

By comparing communication patterns across dimensions, policy administrators can then select the group or combination of groups that is most suitable for the circumstances. While this grouping exercise is an important step, it is a step that can be revisited as circumstances change.

Step 3: Define and test allow-list policies. Armed with an initial schema for grouping endpoints, policy administrators can transition to defining allow-list policies for each group based on its historical traffic flow. Since policies start out in visibility mode rather than enforcement mode, an advisable strategy is to start with the most restrictive allow-list policies and monitor the traffic flows that would be blocked if in enforcement mode based on actual traffic. This strategy allows administrators to balance the risk of disrupting legitimate business operations versus the risk of leaving a communication pathway open for threat actors to traverse before moving policies from visibility mode to enforcement mode.

Worth remembering with this strategy is that even if policies were set to allow all historical traffic flows regardless of frequency, traffic flows that were not present would be blocked once in enforcement mode. In other words, threat actors attempting to move from one endpoint to another through a previously dormant communication protocol (e.g., RDP) would automatically be blocked. The lateral movement would be stopped before it could start. The same would occur with application access policies. Access to applications that were previously unseen and not explicitly included in the allow-list policy would be prevented.

Step 4: Enforce allow-list policies. Once policy administrators are satisfied with the testing of groups and their allow-list policies, the next step is enforcement. For allow-list solutions that leverage the endpoints' native firewall functionality for policy enforcement, this is a push-button task. Each group's allow-list policies are translated into firewall rules; then the rules are broadcast to each endpoint in the group and programmatically applied.

Administrators are not required to be proficient in writing firewall rules. Their responsibility is to define access for the allow-list policies that support business needs and limit threat actors' range of motion.

Allow-list policies will not disrupt end users. If an end-user device is infected and the ransomware attempts to move laterally, it will be blocked — with no impact to the business or end-user experience. The same applies to application environments.

Step 5: Refine allow-list policies. On a continuous basis, policy administrators can refine allow-list policies to accommodate changes in business circumstances (e.g., introduction of a new SaaS application) and to improve the efficiency of policies in blocking threat actors' lateral movement and attempted application access. In addition, as the history of monitored traffic flows lengthens, allow-list policies and/or groups can be added to accommodate seasonality, particularly in application access.

Benefits

The benefits of an allow-list approach fall into three categories: visibility, security, and operations.

Visibility. An allow-list approach fills the visibility gap for organizations lacking a comprehensive and granular view into actual traffic flows and application access. This visibility not only drives improved security but also presents authentic views for network administrators, application owners, and business leaders on actual use of network resources and applications. In addition, prior to and during periods of change, such as transitioning to hybrid work arrangements post-pandemic and migrating from an on-premises application to a SaaS application, changes in traffic flows can be better anticipated and accommodated to ensure smooth transitions and migrations.

Security. Built on the foundation of allowing only what is explicitly defined, an allow-list approach can improve security efficacy in multiple ways, including:

- Restricting the spread of malware by reducing the communication channels for malware to exploit regardless of location (on network or remote)
- Limiting ransomware's potentially crippling impact to the first infected device and, if the threat actor is successful in locating an allowed communication channel, only the devices within the same group

- Reducing the blast radius in zero-day attacks and thwarting the lateral movement of malicious insiders
- Facilitating rapid deployment of host-based micro-segmentation for application access, independent of application and user location
- Decreasing data exposure potential and fortifying compliance with data privacy regulations

Operations. An allow-list approach can accelerate zero trust and micro-segmentation initiatives without any changes or additions to existing network infrastructure. Additional benefits include the following:

- Minimizing new skill development among endpoint management and security teams as the allow-list software agent can be deployed and installed on endpoints through current software deployment methods and firewall rule writing is transparently completed for security teams within the allow-list platform (They do not need to be proficient in firewall rules or native firewall functionality to be proficient in using the allow-list platform.)
- As a cloud-based platform, accelerating implementation, scaling as needed, and ensuring management reliability are inherent attributes
- Limiting investment to a single allow-list solution to control both traffic flows and application access independent of device and application location
- Reducing alert volume as alerts triggered by detection of abnormal activity are structurally eliminated as abnormal activity is blocked by allow-list policies (i.e., not included in allow list) (As the blocked abnormal activity is collected by the allow-list platform, this telemetry can be reused to augment threat investigation and hunting [i.e., indicators of compromise]).

Considering Illumio

Illumio leverages its end-to-end segmentation technologies to offer a flexible allow-list approach. With Illumio's lightweight software agent and cloud-based visibility and administration platform, customers can granularly define and control both traffic flows into managed endpoints and outbound application access.

In host-based fashion, Illumio functions across network infrastructure, application environments, and endpoint locations. Moreover, with Illumio-equipped endpoints functioning as the sensory points for collecting traffic flow data and as the enforcement points for group-based, allow-list policies, no physical or logical modifications to customers' network infrastructure and application environments are required. In addition, Illumio endpoint security coexists with and augments the preventive capabilities of EPP and containment intent of EDR.

Time to value for Illumio customers is short. Although Illumio recommends gathering 30 days of endpoint traffic from which to craft and monitor allow-list policies, customers can proceed at a pace of their choosing.

Tightly aligned with the principles of zero trust and micro-segmentation, Illumio is positioned as a security solution. Yet, day-to-day operations do not require experienced security personnel. It is enough for network and IT personnel to have a functional understanding of zero trust, micro-segmentation, and communication protocols and ports.

Further, Illumio endpoint visibility capabilities provide a single point of truth on endpoint traffic flows. Whether operational personnel are on security, IT, or network teams, they all have access to the same visibility into traffic flows that were permitted and flows that were blocked.

Challenges

The principal challenge for Illumio is in familiarizing network and IT teams with a non-infrastructure-based approach to security. Illumio's approach is different, but being different erases the time, cost, and complexity typically associated with an infrastructure-based approach. Secondarily, allow-list policies (i.e., allow only specific traffic flows and block all others) can face headwinds from personnel who have seen past allow-list initiatives fail and/or view the risk of disrupting critical business operations as too great. Illumio's visibility, drawn from actual traffic flows, policy monitoring mode, and group-based policy creation, will assist in converting skeptics.

Conclusion

Organizations are struggling to manage their cyber-risk. As the number of ransomware attacks, phishing exploits, and security breaches continues to rise, evidence is growing that current endpoint protection and EDR technologies are insufficient. Increasingly diverse, dispersed, and volatile digital footprints are only contributing to vulnerability and risk. With this dynamic, organizations frequently find themselves partially blind to the full extent of traffic flows among their endpoints and applications. In organizations that lack comprehensive, authentic, and real-time visibility, controlling traffic flows for legitimate business needs and limiting communication channels where threat actors hide are reactive trial-and-error exercises. Illumio offers organizations an infrastructure-agnostic solution that eliminates visibility gaps and provides effective allow-list (zero trust) policy controls where threat actors invariably strike first — endpoints.

With mounting threats targeting endpoints, organizations need to strengthen their approach to preventing lateral movement.

About the Analyst

Michael Suby, *Research Vice President, Security and Trust*

Michael Suby is a Research Vice President in IDC's Security and Trust research discipline. In this role, Mr. Suby concentrates on endpoint security and, in collaboration with IDC team members, engages in research spanning a wide and evolving spectrum of security and trust topics.

MESSAGE FROM THE SPONSOR

About Illumio

Illumio, the pioneer and a market leader of Zero Trust Segmentation, stops breaches from becoming cyber disasters. Illumio Core and Illumio Edge automate policy enforcement to stop cyberattacks and ransomware from spreading across applications, containers, clouds, data centers, and endpoints. By combining intelligent visibility to detect threats with security enforcement achieved in minutes, Illumio enables the world's leading organizations to strengthen their cyber resiliency and reduce risk. For more information, visit www.illumio.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com