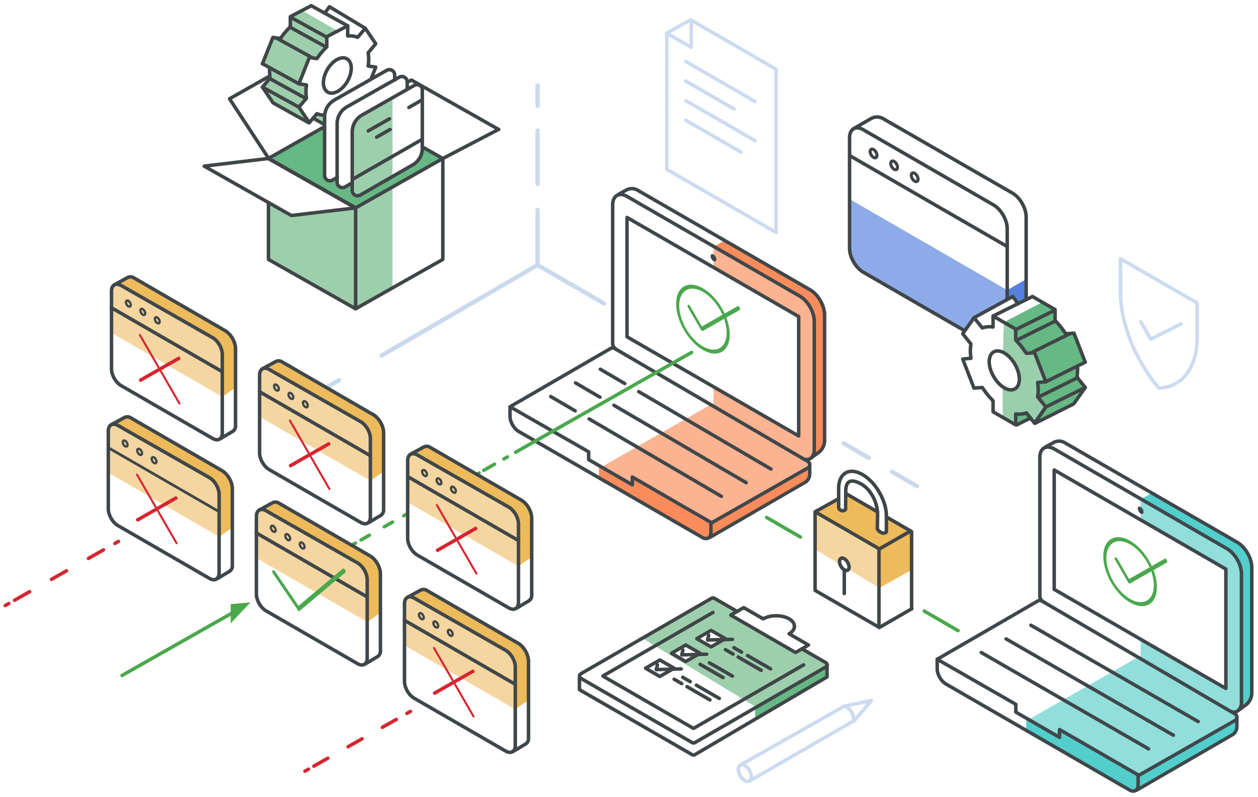
illumio

RESEARCH REPORT



Endpoint Security Effectiveness

How organizations protect their endpoints against ransomware and malware

Endpoint tipping point

Hear us out: attacks either begin on an endpoint or are headed to one.

Why do we make this argument? As has been documented with nearly all ransomware, employees and end users are often the easiest way into an enterprise, large or small, via phishing schemes or malspam. Getting just one user in an organization to open a malicious attachment on their endpoint can be a weak link in your carefully executed security strategy.

At that point, attackers have a foothold on a single laptop, establish persistence, and begin to move laterally – this is how a single infection becomes a full-scale breach.

Least privilege and Zero Trust approaches are global best practices to contain threats. However, the Zero Trust discussion has centered on campus networks, clouds, and data centers – but not yet endpoints, the place where attacks begin.

We wanted to get a sense for how organizations view the effectiveness of their endpoint security, given the disastrous results that can come from ransomware and malware spreading in an enterprise (more on this to come).

Illumio teamed up with Virtual Intelligence Briefing (ViB), an interactive online community focused on emerging through rapid growth stage technologies. ViB's community is comprised of more than 1.2M IT practitioners and decision makers who share their opinions by engaging in sophisticated surveys across IT domains including information security.

This report sums up our findings, with insights into endpoint security efforts, detection adequacy, and the key gap that needs to be addressed.

What did we learn, in a nutshell?

Organizations are indeed dealing with many of the tactics, techniques, and procedures (TTPs) of today's sophisticated and varied ransomware attacks.

Most respondents have updated their endpoint security to include endpoint detection and response (EDR) capabilities.

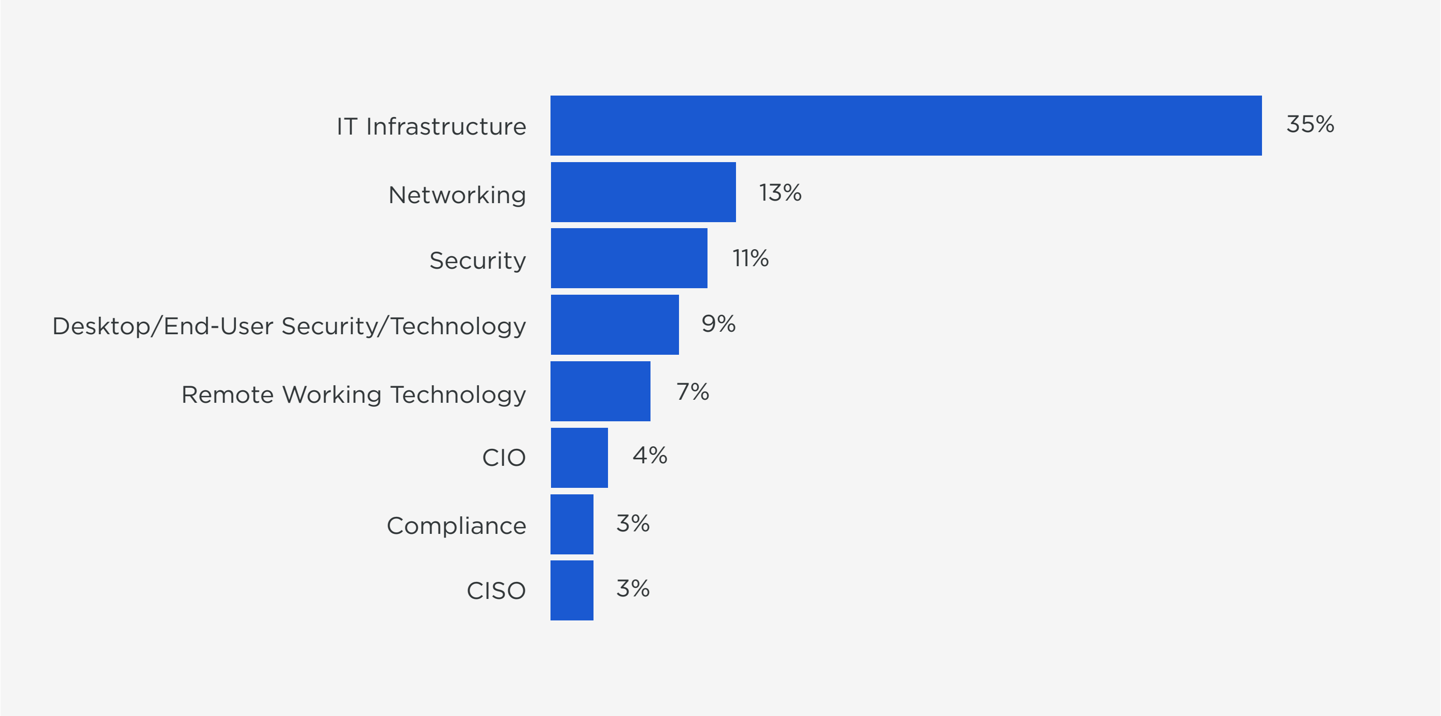
The majority of respondents admit that their endpoint security does not stop everything, and that it needs some time to detect malicious files.

Once breached, there is limited means to contain malware that has gotten in.

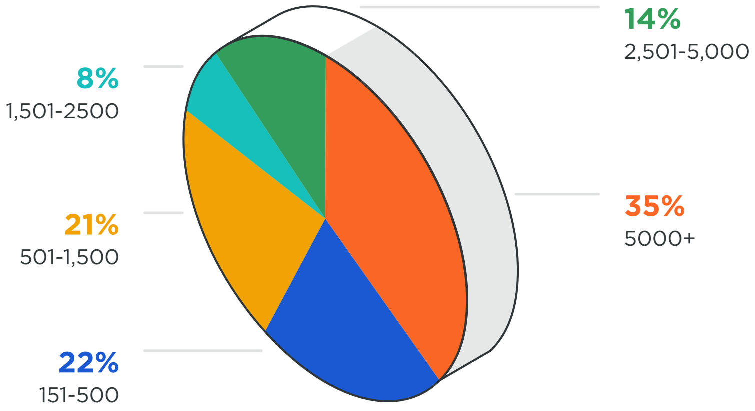
Who did we talk to?

We spoke to 461 IT and security professionals from a cross-section of mid- to large-sized companies, with 57% from companies with over 1,500 employees.

JOB ROLE



COMPANY SIZE



Easy money

Why do attacks keep targeting endpoints?
In two words: easy money.

> Ransomware and malware attacks are lucrative, the fallout is considerable, and attacks will continue to happen.

In 2017, the FBI estimated the total amount of ransomware payments approached $1 billion annually. New estimates suggest global ransomware damages will reach $20 billion by 2021 due to the profitable nature of attacks, according to Cybersecurity Ventures.

It turns out attackers are not religious about filing tax returns nor are companies eager to disclose a major attack – unless they have no alternative. This means the total economic fallout is likely under-reported. This may change as some ransomware attacks now lock up systems after exfiltrating sensitive data, forcing more corporations into fighting public extortion battles over payment.

The attacks we must deal with

Ransomware is a volume business. It's more lucrative to ransom an entire fleet of laptops or a whole network segment than a single system. For this reason, malware and attackers use lateral movement as a key technique to propagate across enterprise endpoints. Over the past few years, we have seen different types of attacks evolve that include lateral movement, vastly increasing the scope of a breach beyond the first infected endpoint. Let's look at a couple of common ones.

Automated ransomware: This is ransomware designed to move laterally on its own, once inside, and is sometimes referred to as a "ransomworm." You should be familiar with it, not just due to the headlines WannaCry and NotPetya generated, but also because of the patches and warnings published by Microsoft and security vendors.

The truth is these attacks were staggeringly effective and fast. It has been reported that a large bank in Ukraine saw its network locked up in (drumroll) 45 seconds with NotPetya. Maersk, a global logistics company, saw its global IT infrastructure crumble in 7 minutes.

How did they move so fast? They propagated peer-to-peer since there were no internal barriers or endpoint segmentation to prevent lateral movement. You may recall how WannaCry spread laterally: via SMB file shares on TCP ports 137, 139, 445.

Attacker-controlled, LotL: Attacker-controlled, living off the land (LotL) attacks don't move as quickly as ransomware with lateral movement built-in, but they are just as devastating due to long dwell time for surveilling an environment. US municipalities have reported a wave of attacks in recent years – many along these lines. In most cases like these, attackers case environments for weeks prior to the ransomware encryption.

These attacks gain a foothold via phishing or brute-forcing poorly configured services like Remote Desktop Protocol (RDP) used for remote access to Windows. Once inside, attacks are methodical, attempting peer-to-peer lateral movement via open ports, for example exploiting RDP or WMI, to ideally reach a domain controller.

Credential harvesting, a thorn in security's collective side, is also used to move laterally. Tools like Mimikatz facilitate this, allowing for privilege escalation, so attackers have greater levels of permission in the network.

Either way, attackers often reach domain controllers, making them an IT admin in the company they are attacking.

At this point they continue to ''live off the land" leveraging existing IT administrative frameworks like PsExec, used to execute processes on other systems, or PowerShell, used to automate operating system management tasks, to drop malicious files onto systems. Some attacks may apply double extortion, by exfiltrating sensitive data before encrypting. Not only are systems locked up, but the sensitive information can be leaked publicly unless victims pay up, amounting to additional pressure for organizations to pay ransoms.

What attacks have (hopefully) been addressed?

What do these attacks have in common? Lateral movement that sees attacks go from the first infected system to as many as possible. Preventing this has now become a key aspect of defense-in-depth. We asked survey respondents the types of attacks they have accounted for in their security today, below.

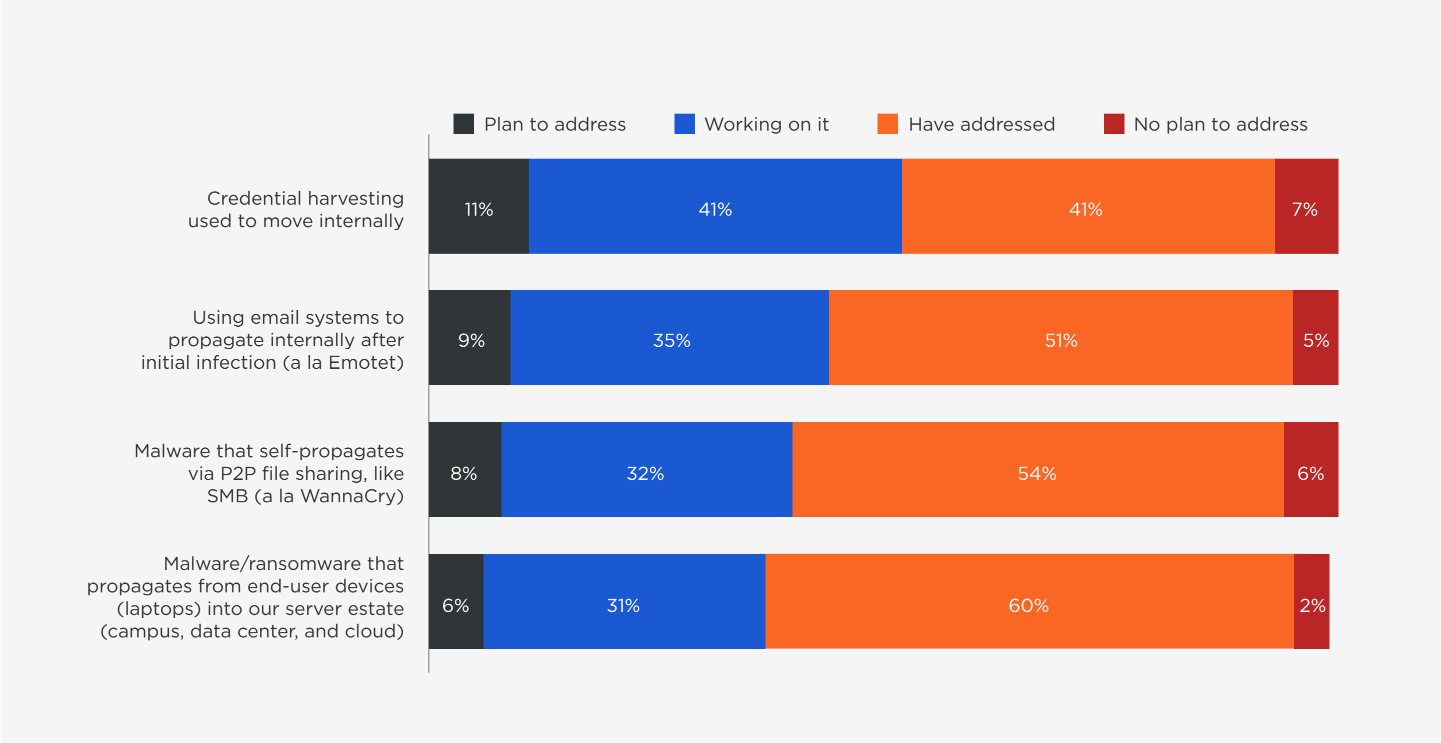
Despite that global scare that WannaCry and NotPetya prompted (or perhaps we should say EternalBlue and DoublePulsar), 46% of respondents note they have yet to address self-propagating ransomware and malware.

60% say that they've taken care of malware moving from laptops to servers. That is serious stuff, so let's hope they mean it.

What are people working on currently? Credential harvesting, with 41% of respondents noting that they are actively addressing or planning to address it. Another 41% of respondents feel they have addressed credential harvesting.

We hope that 41% have indeed been able to address this, given how challenging it can be to guard against and how often credential harvesting is used in attacker TTPs.

CURRENT STATUS OF LATERAL MOVEMENT-BASED THREATS



Endpoint security's tall order

Endpoint security has been given a tall order – being entirely effective in stopping all the ransomware and malware used in the attacks we just described, even never-before-seen threats.

Headed in the right direction (kind of)

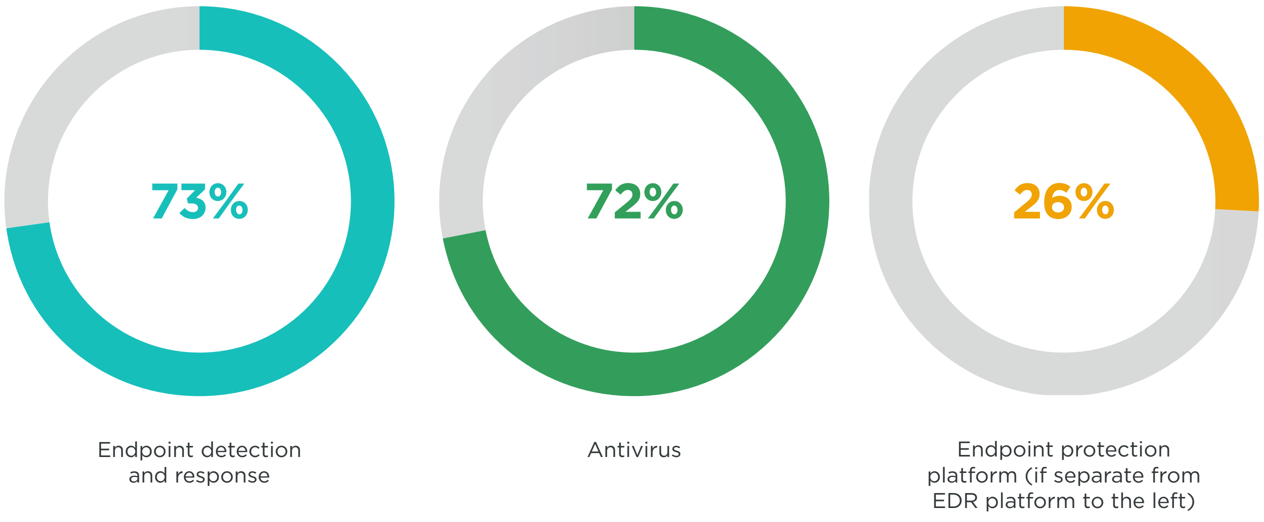
We've seen rapid development in the endpoint security space over the past decade with the rise of next-generation antivirus (NGAV) and endpoint detection and response (EDR) tools. This is imperative to keep pace with fileless attacks or polymorphic malware that changes rapidly and is tested thoroughly by the bad guys prior to being released into the wild.

The antivirus (AV) protection we relied on for years was losing effectiveness in stopping malware. Attackers evaded AV scans that would ostensibly block files from executing by merely adjusting malicious files slightly so they don't match the AV database signatures, thus yielding infections.

For this reason, NGAV and EDR were developed. These tools call on more sophisticated, cloud-delivered malware detection and deep device visibility to account for threats that may not be possible to detect on the initial scan. Once a file is let onto a system, EDR continues to closely monitor both the file and system. EDR can detect malicious activity on endpoints consistent with malware or ransomware: changes to processes, DLLs and registry settings, file and network activity, and so on. If this activity is detected, EDR can retrospectively remove files or isolate systems.

What tools are most relied on today? EDR is the most common at 73%, but respondents also acknowledge they have antivirus capabilities to block all known malicious files. The fact that the majority of respondents have EDR capabilities seems surprising but is likely because vendors they rely on for antivirus have added some EDR capabilities. Whether all capabilities of EDR have been deployed and are functioning is another question.

TOOLS CURRENTLY IN USE

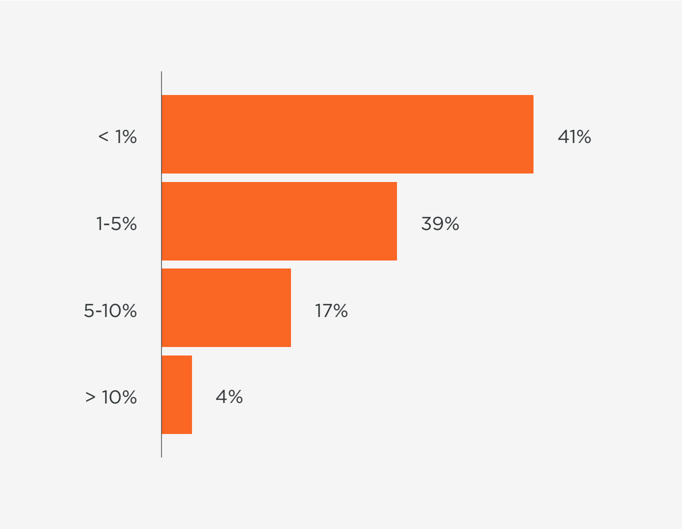


Well, that was fast

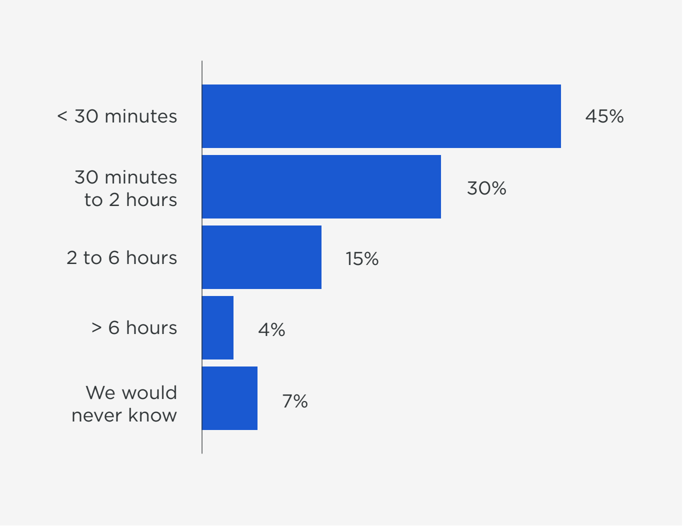
While the majority call on tools like EDR to protect endpoints, we wonder: how effective is this endpoint security? How much malware is missed? If EDR relies on time-to-detection to identify threats, how long does it need?

We asked, and here is what we heard.

ESTIMATION OF MISSED MALWARE



LENGTH OF TIME FROM INITIAL INFECTION TO DETECTION



SURVEY RESPONSES

> "...not sure how long it takes to detect."
>
> "...sometimes it's only detected after it has spread."
>
> "...system detects immediately but response...can be delayed due to escalation, especially off hours."

56% of respondents feel that their endpoint security tools miss between 1 and 10% of malware. That is a real gap to account for. 41% feel it catches nearly everything at <1%, but remember, nearly everything is not everything.

59% of respondents from organizations with more than 5,000 employees feel that their endpoint security will miss between 1 and 10 percent of malware, no less.

How fast is fast enough? That is, how long does EDR need to detect? 45% feel that EDR will detect malware within 30 minutes. Another 30% feel EDR tools need between 30 minutes and two hours.

On one hand, this seems rapid. Malware only has up to two hours to inflict damage. On the other, if attacks like NotPetya took down entire networks in 45 seconds, we'll still need to figure out ways to prevent malware from spreading to backstop tools like antivirus or EDR if they need up to two hours to detect it.

How did you get in here?

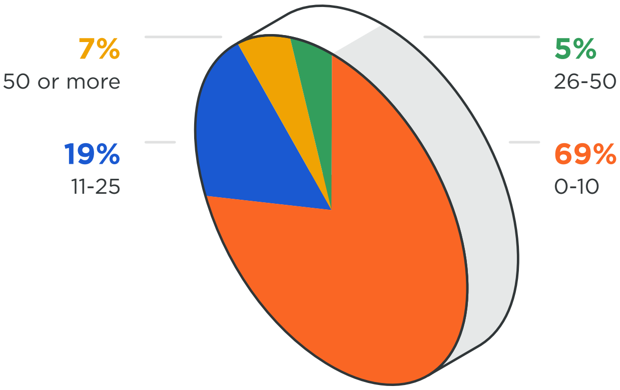
Once malware has gained a foothold, it moves laterally to infect as many laptops or servers as possible. Endpoint security tools aren't perfect, so how do we backstop them to prevent propagation?

We usually don't. At 64% most respondents rely on EDR to isolate the host once malware has been detected, which may take 30 minutes or two hours.

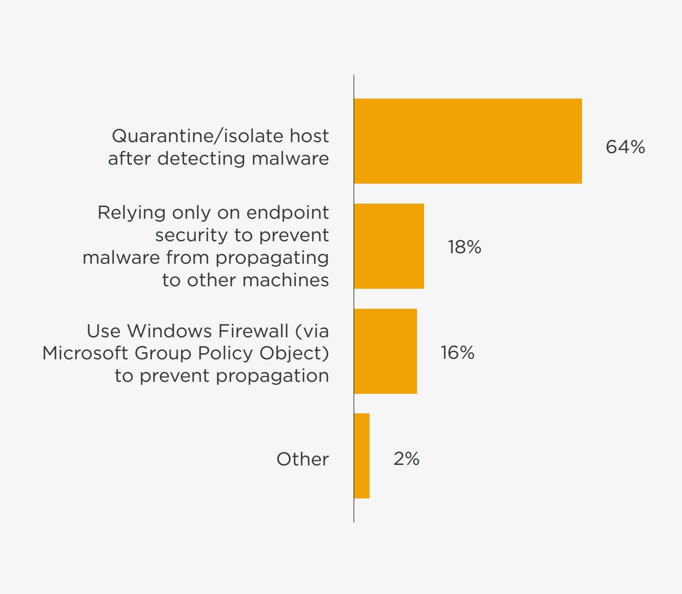
Either way, there is a window of vulnerability in which malware or ransomware can spread. 16% of respondents go to the painstaking effort of creating a Group Policy Object (GPO) to limit lateral movement between laptops.

With nearly 1 in 3 respondents reporting 11+ incidents per week, any missed detection or delay in response could cause rapid escalation.

NUMBER OF INCIDENTS PER WEEK



PREVENT THE COMPROMISE



The endpoint gap to fill

As you've learned in this report, organizations know their endpoint security will occasionally miss malware. We know that malware will then often look to propagate since lateral movement is a key TTP. This could lead to a data breach.

This gap in endpoint protection must be addressed.

This brings into focus the need for additional measures beyond endpoint security tools like NGAV or EDR to stop ransomware and malware from spreading once inside. Fortunately, the need to stop credential-based attacks is also generating considerable attention from the security industry given their gravity.

Organizations are best served with modern endpoint security, whether NGAV, EDR, or both, designed to detect and stop malware. Since no security technology is 100% effective, we must fill this gap with additional endpoint security capabilities meant to stop the lateral spread of ransomware and malware for additional risk mitigation.

This is where Zero Trust comes back into the discussion. Add Zero Trust, eliminate lateral movement. That's its purpose. And it's time to bring it to the endpoint.

Need help getting started? Learn how Illumio makes endpoint Zero Trust possible (and easy).

Illumio enables organizations to realize a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any endpoint, data center or cloud. Founded in 2013, the world's largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085, Tel (669) 800-5000, www.illumio.com.