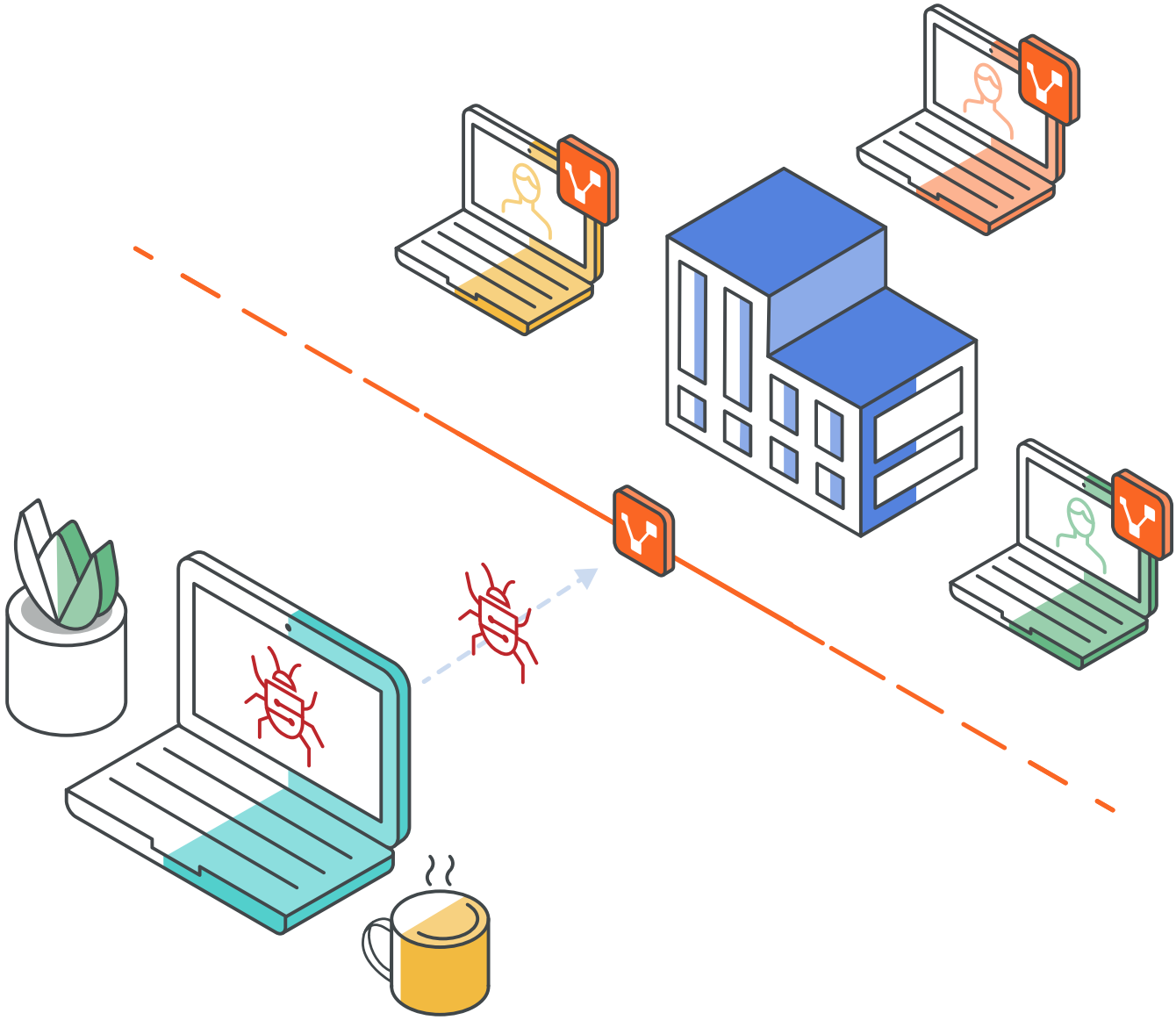
illumio

RESEARCH REPORT



Security Risks 2021: Ransomware and the Return to the Office

How organizations are securing remote endpoints in a hybrid work world

Introduction

The world underwent a sweeping shift to remote work for much of 2020. In 2021, the future will likely be a flexible hybrid model. Many businesses face a return to socially distanced on-site operations with employees rotating into the office a couple of days a week. But as we plan for a future return to the office, how do we know what's been happening on employees' private networks while they work from home? And what is our workforce bringing back to the campus network?

2021 will force us to account for the security risks in this hybrid work model.

This report will examine remote endpoint security, from the amount of visibility and control IT can exert on employees working from home to how organizations are addressing rapid ransomware attacks that can quickly spread through the enterprise – on or off the campus network.

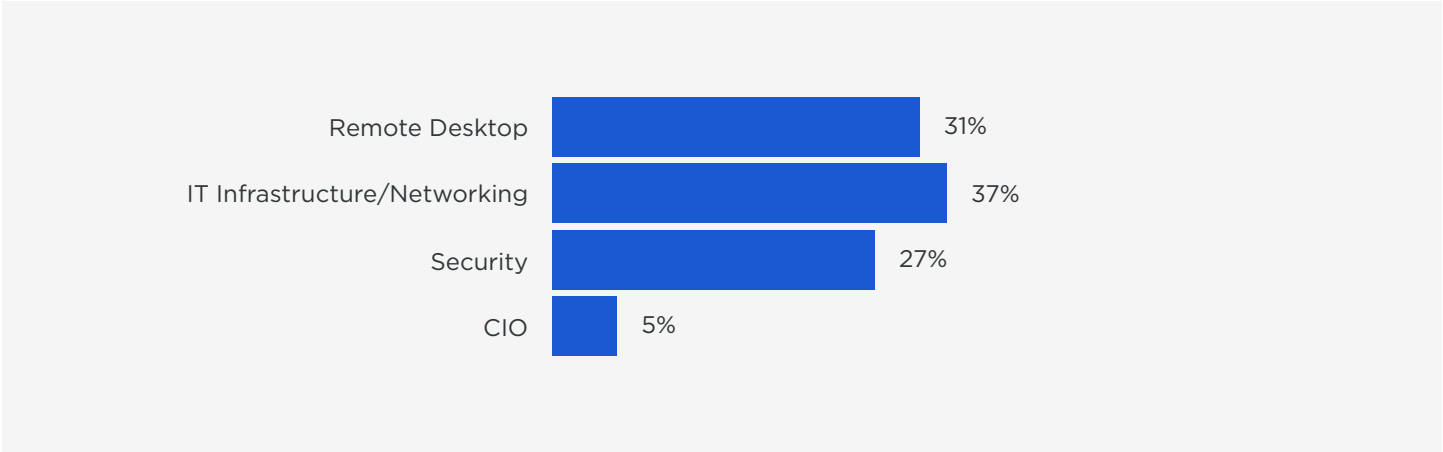
In a nutshell, here are a handful of key findings:

- Organizations lack visibility into what is happening to work devices on home networks, which they previously had on the office network.
- The VPN is considered the primary security and visibility tool for remote employees.
- Many organizations have ransomware recovery plans, but would be willing to pay attackers in a worst-case scenario.
- Pre-emptive Zero Trust controls to prevent attackers or ransomware from moving laterally are not fully embraced to stop inevitable attacks.
- Credential dumping, a prominent attacker technique, is not yet a concern for many enterprises, for better or worse.

Who did we talk to?

We spoke to 344 IT networking/infrastructure, desktop and security professionals from a cross-section of mid- to large-sized companies, with 64% from companies with more than 1,000 employees. All respondents have responsibility for infrastructure, security, and remote desktop operations.

JOB ROLE BY FUNCTION



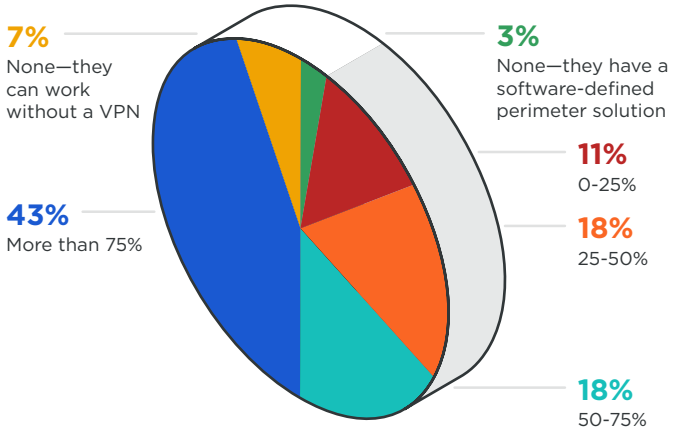
illumio

Where's the remote control (of employee endpoints)?

In reality, employees have been working from home for many years.

For all recent talk of software-defined perimeters or Secure Access Services Edge (SASE), VPNs remain the first choice for offering employees remote access, with 61% of respondents noting at least half their remote employees must use a VPN.

What percentage of your remote employees must use a VPN to work?



Scaling up VPNs was the only choice for most organizations as a response to the increase in remote workers. Fifteen years ago, the results would have been close to 100 percent of organizations using VPNs, but the growth of SaaS-delivered applications and cloud-based office productivity tools has shifted the results. The reality is that connecting to the office via a VPN and then accessing cloud apps through a gateway is a poor user experience.

One of the perceived issues for home workers is the lack of visibility into the remote device and home network. There are privacy issues related to companies being able to see traffic on the home network, so being able to control what enters and leaves the company laptop is paramount.

One of the main threats for devices at home is from other devices on the same network.

How much visibility do you have into remote user endpoints?

66%
have the same level of visibility for users on the VPN as for users at the office.

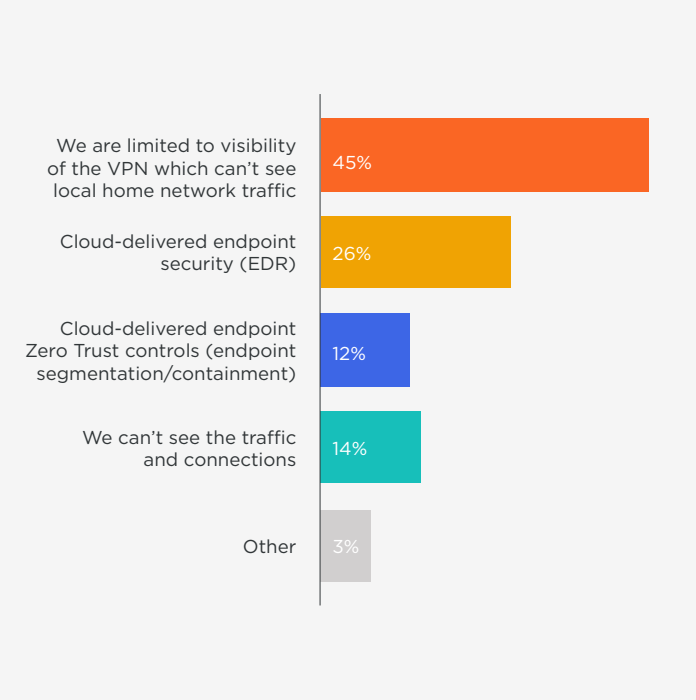
10%
said that they achieve visibility with cloud-based tools.

16%
say they have less visibility.

illumio

Going a step further on visibility, we wanted to know how much understanding employers have of what is happening on employee home networks.

How do you get visibility into connections to work laptops on home networks?



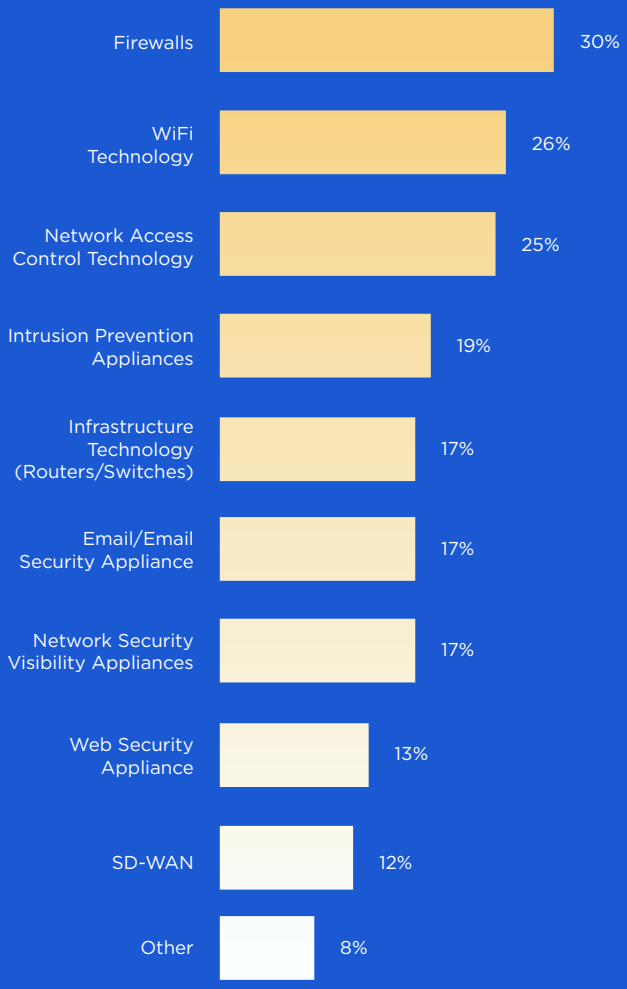
The reality of this is that 59% of respondents cannot see attempted connections from other devices on the home network. This should be a major concern to most organizations because devices on home networks are vulnerable to peer-to-peer (P2P) and lateral attacks. These potentially compromised devices will then connect to the corporate network.

Some of the issues around remote access, cloud access, and mobile working will be resolved as SASE replaces traditional VPN solutions, but the issue of potential attacks from the local network will remain.

Unfortunately, compared to visibility on the office network, many organizations are still in the dark, attempting to protect devices they cannot see, making securing employee endpoints difficult.

Pink Slips 2021

These security tools will see less investment with fewer employees in the office.



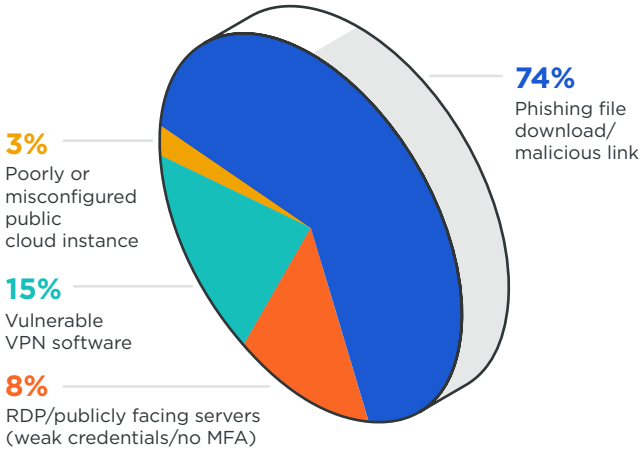
Not surprisingly, hardware appliances that protect campus networks are first in line to have their spending cut. Topping the list are firewalls, WiFi technology, and Network Access Control.

illumio

Threat management

Whatever organizations do to prevent attacks, there is a good chance that we will be the subject of a breach attempt. Identifying the initial attack point is key to trying to prevent it from happening to begin with.

What initial attack vector is of most concern?



Phishing is always likely to be the greatest concern as it is the vector where we have the least control, given end users are involved. But the other concerns should not be ignored. It is interesting to see the worry about vulnerable VPN software even though many attacks have come via public-facing servers and portals.

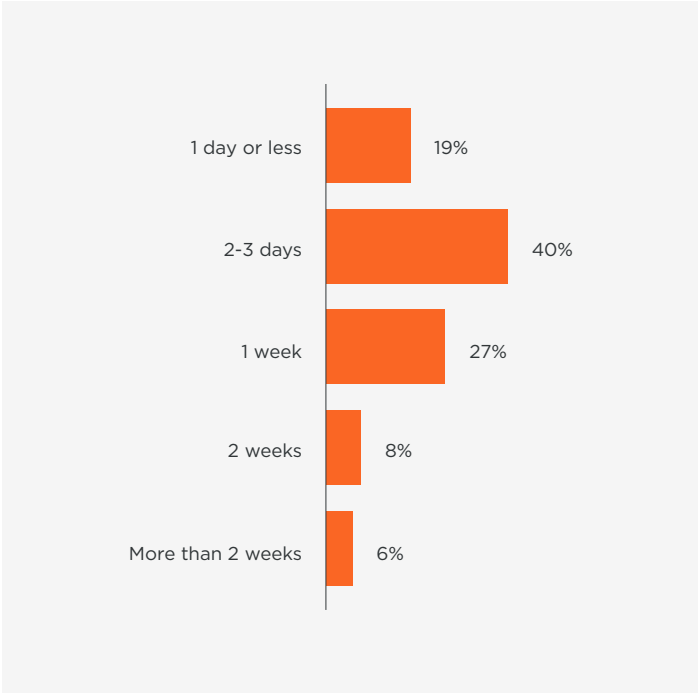
"Rapid" ransomware response

Most organizations would be in a bind in the event of a broad security incident. So how – and how quickly – could they get back on track in the event of a ransomware attack?

More than half, 53%, will call on backups to restore systems. Another 41% will reimage machines; 2% would plan to pay the ransom.

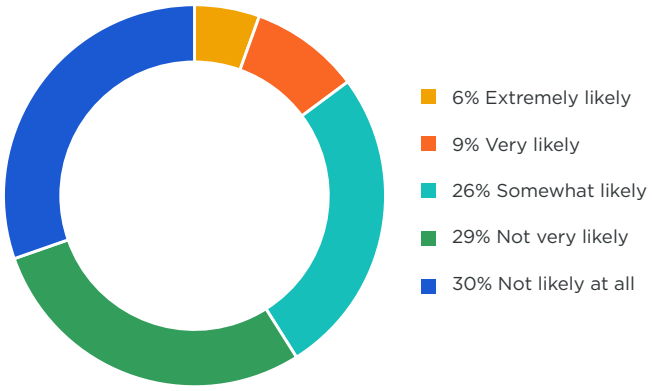
As for how long it would take, the vast majority, 81%, would need at least two to three days to recover – likely operating at less than a quarter of their normal capacity.

How much time would you need to recover from a ransomware attack?



We asked respondents if they would consider paying the ransom if they could not recover in the required time.

How likely are you to pay the ransom to recover data?



41% acknowledged they would be somewhat likely to extremely likely to consider paying – and with those odds of victims playing profitable ball with attackers, ransomware is unlikely to go away anytime soon.

From bad to worse?

Attackers in many recent breaches moved laterally between endpoints and workloads to further the attack. Solving this problem can potentially halt the breach or at least reduce the impact.

We asked our respondents how they stop ransomware from moving between laptops.

Very few put preventive, "Zero Trust" controls in place to proactively contain lateral movement or the spread of ransomware. Instead, they rely on endpoint security (next-generation anti-virus, endpoint detection and response, etc.) to block ransomware from executing to begin with.

74%
expect endpoint security to block every initial attack or detect malicious behavior and isolate the infected endpoint after detection.

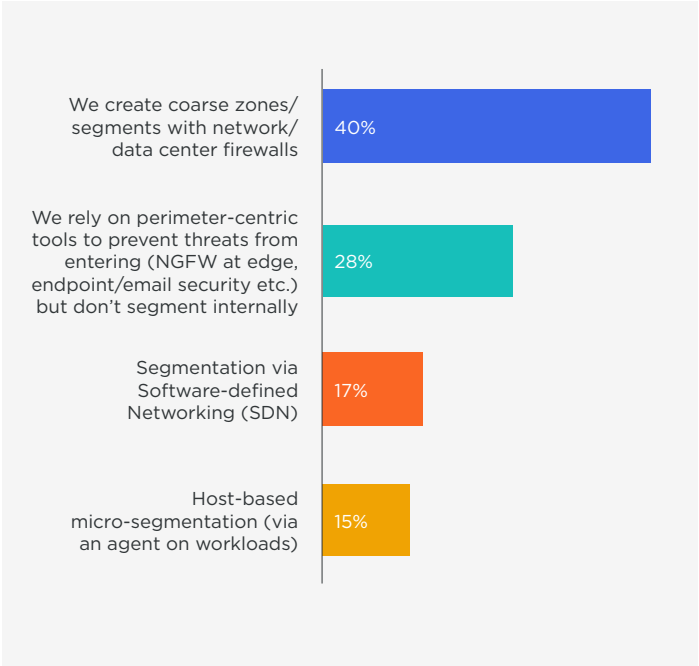
25%
called on Group Policy Objects or endpoint firewall controls to prevent the spread of ransomware.

The challenge? Technologies sometimes miss threats – and by the time they have been detected, attackers have had time to move throughout the environment.

Modern endpoint security tools are very good at catching most threats, but we can't assume they will catch every threat or piece of ransomware every time.

What about when crown jewel applications and data are at stake in the cloud and data center? Do organizations use segmentation or micro-segmentation, a critical Zero Trust control, to prevent lateral movement?

How do you stop ransomware from moving between data center and cloud workloads?



Many use firewalls to create coarse zones between areas like the user/campus zone, data center, and DMZ. This means if there is a compromise in any zone, attackers can reach every workload or server inside it. Respondents resort to familiar, traditional security techniques to solve what is becoming a very sophisticated problem.

More than a quarter of respondents, 28%, acknowledge they have no segmentation, that is, totally flat networks.

There are some key requirements for the level of segmentation required to solve this problem:

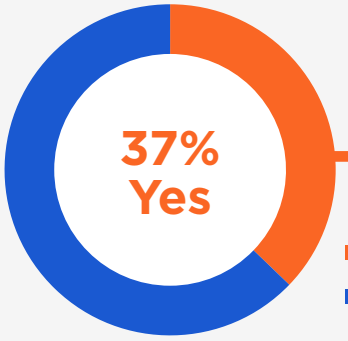
1. Real-time visibility
2. Simple policy creation
3. Dynamic workload enforcement

It is not possible to achieve these factors using firewalls, SDNs or perimeter-centric tools as they are not close enough to workloads and do not provide a real-time view of applications and their flows.

Assume Breach?

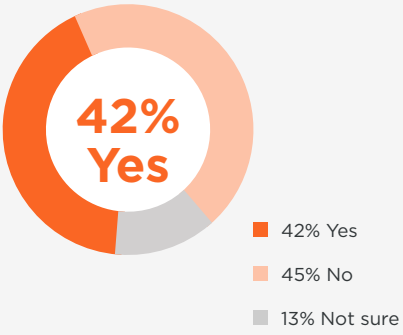
The MITRE ATT&CK® framework has become an indispensable resource for security pros seeking to learn about the tactics and techniques attackers use in the real world. We were curious to know to what extent security team rely on it for advice and direction about how attackers operate to move inside an environment. The results were lower than anticipated. The results were lower than anticipated with only 16% using the framework to improve their security.

Are you familiar with the MITRE ATT&CK® framework?



Yes

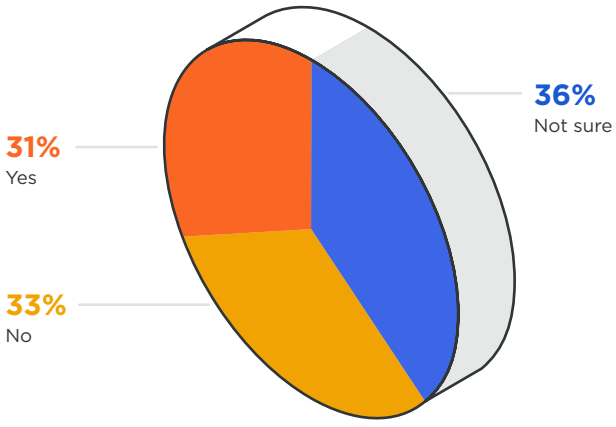
If yes, do you use the framework to inform your security?



It is not just the initial attack vector that is the issue, but what happens next. While many companies try to stop the initial attack, only a few plan for the entire attack chain.

An attacker lateral movement technique prominent in many recent attacks is credential dumping. Credential dumping has been carried out via tools like Mimikatz to steal legitimate credentials from a system's memory to then move laterally throughout an environment. This next question explores that.

Are you concerned about Mimikatz and credential dumping tools?

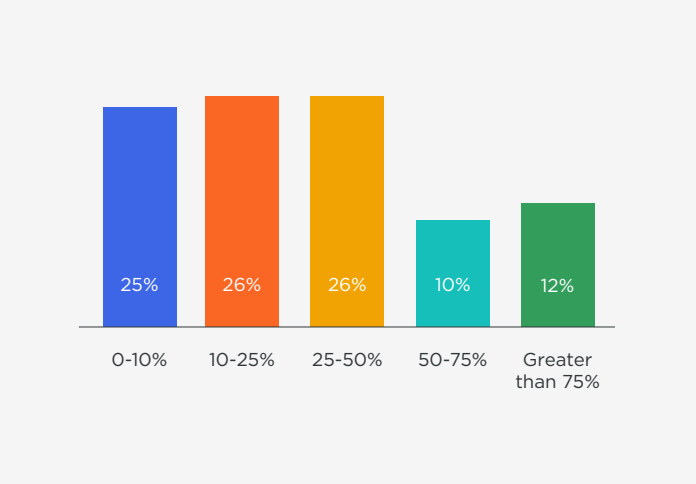


Only 31% are concerned about credential dumping, despite it being a hallmark in many recent attacks.

Impact

Finally, what is the risk we're running with limited endpoint visibility and control? We've seen the growing threat of mass infection from a ransomware incident play out across organizations in the last few years, from hospitals to law firms, to schools, to multinational corporations. Even if they're not forced all the way back to pen and paper, most organizations cannot continue "business as usual" operations without the use of employee laptops due to a security incident. In fact, by the numbers, 51% of respondents would run at one quarter or less capacity if their laptops got infected or ransomed.

At what capacity could your organization run without the use of employee laptops due to a security incident?



While it may be surprising that 22% of organizations could maintain over 50% capacity in the event of losing employees laptops, it is worth remembering that some industries are more reliant than others. Many industries have supported remote services and outsourcing for years or rapidly built new business models to survive in the current climate – and may wonder why they did not do it that way before.

Moving forward

The last 12 months have been like no other in the history of IT. Many employees will continue to work remotely full or part-time in 2021, and even begin to travel – with only a VPN and endpoint security protecting their laptop – and without the control and visibility of the enterprise security stack.

As in 2020, computers will remain at risk on home networks, shared with other laptops, users, and devices. Workers will then connect to the VPN or head into the office, allowing for a threat to potentially move laterally from an infected laptop on a home network to other laptops, servers, and workloads on the corporate network.

It is important to plan for the entire attack life cycle and one of the simplest ways to do that is to segment resources to stop lateral movement between both endpoints and host workloads. Many of the new cybersecurity frameworks around the world like Zero Trust, NIST and NIS-D all require some segmentation of critical data and infrastructure. Being able to do this simply and at scale is going to be a focus for many in 2021.

Illumio has always focused on making segmentation simpler, more powerful and scalable. With Illumio's visibility and host-based segmentation, organizations can see and contain lateral movement of ransomware between endpoints or data center and cloud workloads.

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.

Gartner peerinsights™

See what customers have to say about Illumio.