CROWDSTRIKE

2021

CrowdStrike Global Security Attitude Survey

Table of Contents

Introduction

This report explores the attitude of security professionals focusing on many different areas, including:

- **Why trust in legacy vendors, including Microsoft, continues to fall; the success rates of software supply chain attacks; and whether organizations are taking the necessary action to protect themselves against this vector**

- **How effectively organizations are defending against ransomware; the costs that can be incurred if a ransomware attack is successful; and why ransomware costs are increasing at an alarming rate and why most times they include extortion fees**

- **Why organizations are getting slower at detection, and how close organizations are at meeting CrowdStrike's 1-10-60 benchmark for detecting, investigating and containing a cybersecurity incident**

On the surface, the core aim of a cybersecurity professional is very simple: ensuring their organization is secure by keeping intruders out. But, in reality, there are so many moving parts – both internally and externally – that this objective has become increasingly difficult.

From an external perspective, the cyber threat landscape is always evolving, with well-established attack vectors – such as ransomware and software supply chain attacks – becoming more sophisticated and persistent. In addition, cybercriminals continually improve their tradecraft, using increasingly sophisticated and stealthy techniques like fileless attacks to evade detection and breach the defenses of organizations. It is abundantly clear that cybersecurity teams have their backs against the wall when trying to defend against increasingly sophisticated and complex attacks.

That's only one side of the coin though. Internally IT teams are facing a completely different challenge – one that a couple of years ago nobody could have predicted. Naturally, COVID sent shockwaves around the globe in almost every industry. For those working in IT security, the increased attack surface stemming from the shift to remote and hybrid operating environments changed the way they must secure their organization. Today's world is both remote-first and digitally complex.

Security teams have been swimming upstream since long before the pandemic, though, due to factors such as limited resources and the industry's well-documented skills shortage. Most teams battle thousands of alerts a day and use outdated, legacy technology that is ineffective against today's sophisticated cybercriminals. So, with these mitigating circumstances in mind, it's easy to understand why there have been so many high-profile breaches in recent years.

Taking all of these different elements working against organizations into account, clearly the time is now for security teams to take the necessary steps to reduce their chances of being the next victim of opportunistic cybercriminals and well-equipped state-sponsored adversaries. Transforming security infrastructure is imperative if businesses hope to avoid the financial and reputational harm caused by a successful cyberattack. The businesses that embrace cloud-first, modern technologies such as endpoint detection and response (EDR), extended detection and response (XDR), Zero Trust, and human-empowered managed threat hunting and intelligence will be the ones able to solve the fundamental challenges to thrive in the heightened threat environment. As adversaries advance their tradecraft to bypass legacy security solutions and exploit trusted technologies, the combination of world-class technology combined with expert threat hunters is mandatory to detect and prevent today's sophisticated threats.

Key Findings

63%

of respondents admit that their organization is **losing trust in suppliers, such as Microsoft,** due to frequent security incidents

84%

believe that **software supply chain attacks could become one of the biggest cyber threats** to organizations like theirs within the next three years

Only 36%

have **vetted all new and existing suppliers** for security purposes in the last 12 months

45%

of respondents' organizations **experienced at least one software supply chain attack** in the last 12 months, compared to 32% in 2018

The average ransom payment increased by **63% in 2021 to $1.79 million (USD)**, compared to **$1.10 million (USD) in 2020.** ***CrowdStrike Intelligence*** has observed the average ransom demand from attackers is **$6 million.** While attackers aren't getting quite the amounts they are seeking, they are still earning massive payouts. CrowdStrike attributes this to companies understanding both the threat and their exposure, and their ability to negotiate with attackers.

96%

of those who paid the initial ransom **also had to pay extortion fees**

66%

of respondents' organizations **suffered at least one ransomware attack** in the past 12 months

57%

of those hit by ransomware **didn't have a comprehensive strategy in place** to coordinate their response

On average

respondents estimate that it would take their organization **146 hours to detect a cybersecurity incident**, compared to 117 hours in 2020, and 120 hours in 2019

On top of detection time

it's estimated that organizations would need **11 hours** to triage, investigate and understand an incident, and **16 hours** to contain and remediate, on average

69%

have suffered a **cybersecurity incident** as a **direct result of teams working remotely**

Organizations Are Facing a Crisis of Trust in Microsoft and Other Legacy IT Vendors as Software Supply Chain Attacks Show No Signs of Slowing Down

Software supply chain attacks have become more prolific, with the Sunburst and Kaseya attacks being among the most headline-grabbing in recent years. The escalation in software supply chain attacks is supported by the fact that 77% of respondents report that their organization has experienced this type of attack in the past, increasing from 66% in 2018. Additionally, 45% of respondents reported that their organization suffered from a software supply chain attack in the last 12 months rising from 32% in 2018 .

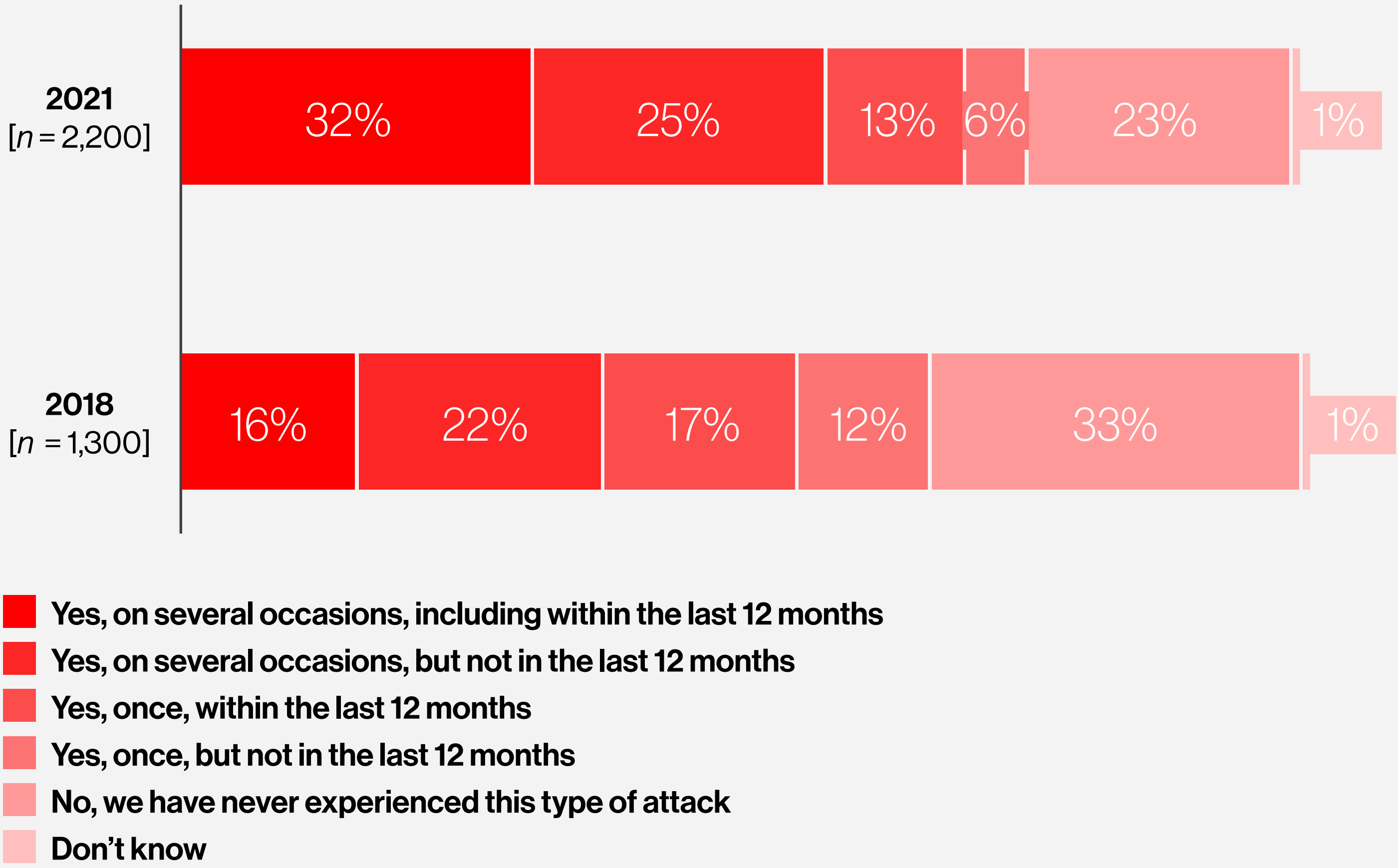

Figure 1: Has your organization ever experienced a software supply chain attack?

For cybercriminals, the beauty of software supply chain attacks is that while the initial objective of infiltrating a single company remains the same, their chances of impacting hundreds if not thousands of other businesses are significantly higher due to what their primary target specializes in.

So, considering that non-software companies don't have complete control when it comes to defending against software supply chain attacks, it's essential that they have an action plan for responding to such a breach when it occurs. Although these strategies aren't always common — almost six in ten (59%) concede that when their organization suffered their first software supply chain attack, they did not have a comprehensive strategy in place to coordinate their response.

63%

of respondents say their organization is facing a crisis of trust in legacy IT vendors, such as Microsoft, due to frequent security incidents

This must change if these companies want to limit the damages, should they be on the receiving end of such an attack. And although they do relinquish some of the power when it comes to defending against this vector, they are not totally hamstrung. To do their due diligence, they must subject all businesses in their supply chain – software or otherwise – to rigorous vetting procedures.

But IT vendors must also shoulder some of the responsibility as they are the first line of defense against this form of cyberattack. This is particularly true of legacy vendors who are ingrained in the infrastructure of businesses worldwide – if changes are not made, then trust in these brands will begin to nosedive. According to 63% of respondents, their organization is facing a crisis of trust in legacy IT vendors, such as Microsoft, due to frequent security incidents.

However, only 36% of respondents can claim that all of their organization's software suppliers, new or existing, have been vetted for security purposes in the last 12 months. This is only a slight increase on the 32% reporting the same in 2018. Taking into account the way in which supply chains have grown in recent years, and the increased dependence on these supply lines during the pandemic, despite the slight rise in the percentage vetting all suppliers, it still feels like something of a backward step.

There is also a level of over-confidence from organizations in their supply chains, with 93% of respondents reporting that they have total or moderate confidence in the IT security of their organization's suppliers. Further, a similar proportion (91%) have this same level of confidence in their organization's suppliers' supply chain security. These confidence levels are misplaced. If organizations do not begin to take more responsibility for thoroughly vetting all of their external suppliers and holding them to the same security standards as they hold themselves – something that 72% admit isn't always the case – their chances of being breached are only going to increase.

84%

of those surveyed believe that software supply chain attacks have the potential to become one of the biggest cyber threats to organizations like theirs within the next three years

Perhaps most concerning of all for respondents' organizations is that 84% of those surveyed believe that software supply chain attacks have the potential to become one of the biggest cyber threats to organizations like theirs within the next three years. This clearly reinforces the need to revisit their vetting procedures and their recovery strategies because if software supply chain attacks do become even more prevalent in the coming years, then organizations could find themselves in deep water.

It also demonstrates the need for a holistic approach when it comes to defending against software supply chain attacks – technology giants such as Microsoft are not immune to this form of cyberattack, and rather they are the gateway onto the network for millions of organizations around the globe. If they do not hold themselves accountable, then many others could suffer.

But, it is also important that individual companies do their due diligence when trying to defend against, and recover from, this type of attack. This means ensuring the thorough vetting of all suppliers, and the implementation of a comprehensive recovery strategy to coordinate their response if such an incident occurs.

Today's threat environment and the supply chain attack vector highlights the need for organizations around the world to transform their security and adopt a Zero Trust architecture in order to protect their digital assets, identities and core infrastructure as threat actors are well resourced and are becoming more sophisticated. Organizations at all levels of the supply chain must work together to ensure they don't collectively become the next victims of the cybercriminals executing these attacks.

Ransomware Remains a Persistent Threat, with Costs and Extortion Fees on the Rise

Over the last two years, much has changed for organizations around the globe, but one thing that has remained a constant is the danger posed by ransomware attacks. Arguably, this vector has been the most successful type of cyberattack in recent memory. And, with cybersecurity teams still adjusting as they aim to set up and secure hybrid working environments for the future, it stands to reason that those perpetrating these attacks will continue to see high levels of success.

Therefore, it makes sense that ransomware is the attack vector most commonly (44%) reported by respondents to be causing concern when thinking about IT security in their organization over the next 12 months. However, what is slightly surprising is that this proportion has decreased from the 54% reporting the same in 2020 and has fallen back more in line with the figures of 2019 (42%) and 2018 (46%). Perhaps with everything else that was going on in 2020, respondents' levels of concern were heightened, and they were slightly more on edge with regard to ransomware than they otherwise would have been.

An alternative theory could be that IT security teams are becoming more adept at dealing with ransomware attacks – but does this argument really hold any weight?

In short, the answer is a resounding “no,” and it actually appears as though organizations are finding it increasingly difficult to defend against ransomware compared to 12 months ago. Almost two-thirds (66%) of those surveyed admit that their organization has suffered from a ransomware attack in the last 12 months – a notable rise on the 56% saying the same in 2020. What’s more concerning is the fact that 33% have suffered multiple attacks in the past 12 months, compared to 24% last year.

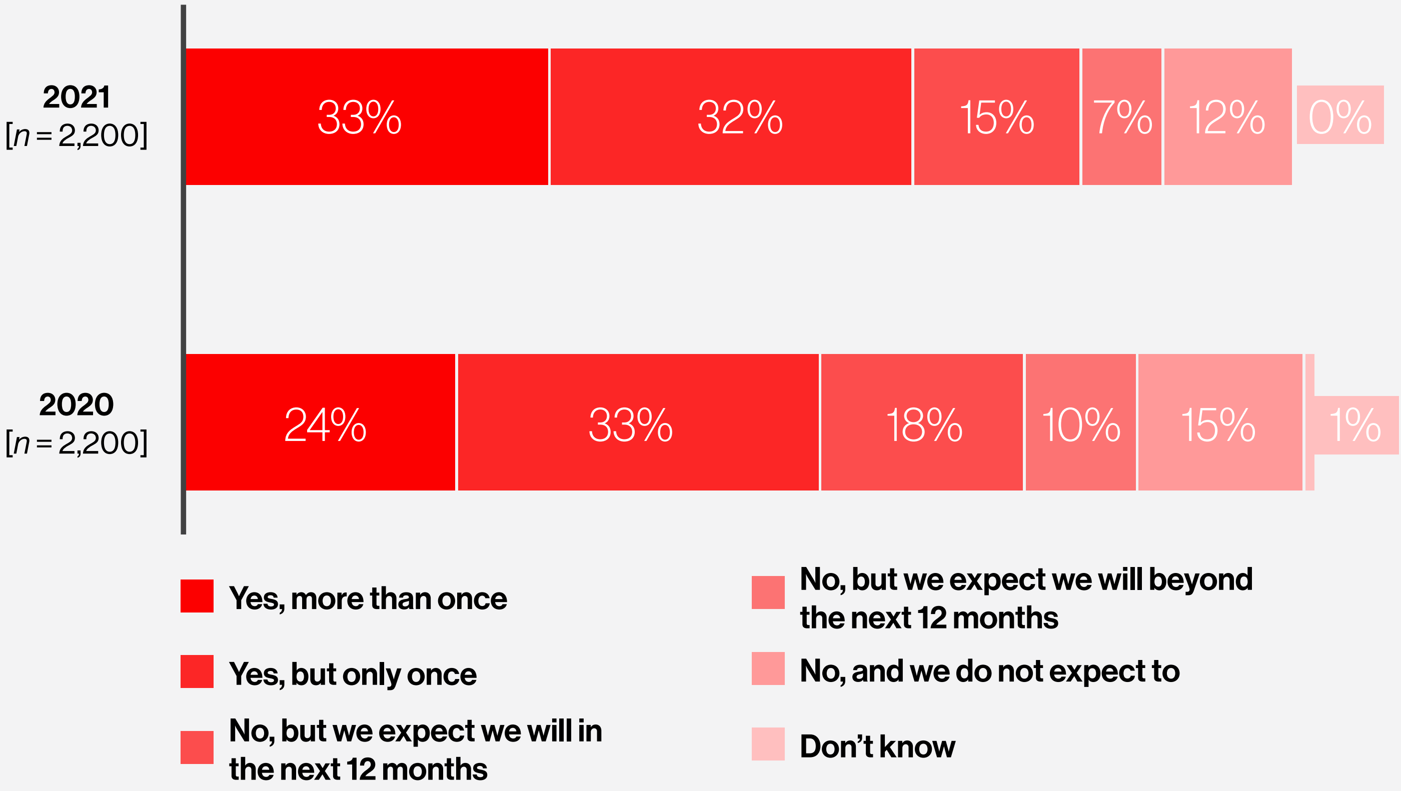

Figure 2: Has your organization suffered from a ransomware attack in the past 12 months (whether you actually paid the ransom or not)?

Whether the ransom is paid or not, these attacks are a drain on resources, and can have significant negative impacts for brand reputation, as well as personal impacts on the employees charged with fighting off a seemingly never-ending barrage of attacks. And this is without even mentioning the possible consequences for the career of an employee who makes a mistake that leads to a successful ransomware breach.

So, while these attacks are based around monetary gains for cybercriminals and can obviously lead to financial ramifications for the business due to regulatory breaches, there are plenty of other wide-reaching impacts that can weigh heavily on organizations and employees alike.

As such, it's critical that these companies make the necessary adjustments when struck by ransomware to try and guard against future incidents. For 60% of respondents' organizations who found themselves in this position over the last 12 months, they upgraded their security software to reduce the risk of future attacks, while 58% upgraded their security staff for the same reason.

But regardless of these positive steps after the event, almost a quarter (24%) ended up paying the ransom, which is a similar proportion to 2020 (27%). However, the ransoms paid over the last 12 months have dramatically increased by nearly 63%. Last year, on average, respondents' organizations were forced into paying $1.10 million (USD), whereas this year the average payment is $1.79 million (USD).

The situation in the Asia Pacific and Japan (APJ) region is most concerning of all, with the average ransom paid at $2.35 million (USD), compared to $1.55 million (USD) and $1.34 million (USD) in the US and Europe, Middle East and Africa (EMEA) regions respectively. Clearly, this type of outlay isn't sustainable for organizations, particularly if they're being targeted by multiple attacks over the course of a year. Also, events like this could quite easily create a period of financial turmoil in any company that is forced into taking this course of action, especially as they are likely to be operating at a reduced level until the compromised endpoints or workloads are fully remediated.

Unfortunately, for **the vast majority (96%)** of those who ended up paying their attackers, the saga didn't end there, as they were also **forced into paying additional extortion fees, equating to $792,493**, on average. These "double extortion" fees alone would be a notable outlay, but on top of an already hefty ransom payment, it could be a devastating blow for many organizations, particularly during a period of economic uncertainty.

But, while these figures are eye-watering, the real surprise – considering the well-known prevalence of ransomware – is that many organizations were underprepared to deal with such an attack. In fact, almost six in ten (57%) of those hit by ransomware in the last year admit that their organization didn't have a comprehensive strategy in place to coordinate their response.

Moving forward, it's imperative that organizations better equip themselves to deal with a ransomware breach because increasingly it seems as though it is a question of "when" rather than "if" they will suffer at the hands of this highly persistent attack vector.

And it isn't just direct attacks against the company itself that IT security teams must contend with when putting together their response strategy. Ransomware can strike anywhere in the supply chain, and when this happens there is evidence to suggest that it might just be easier to pay the ransom to resolve the problem as quickly as possible. Over two-thirds (69%) of those surveyed report that if their organization's software supply chain was the subject of a ransomware attack, and the attacker had encrypted some or all of their critical data, then they would at least consider paying the ransom.

Nevertheless, even if ransomware is now something of an inevitability, and having a recovery strategy is crucial, companies must still proactively seek ways of minimizing their chances of becoming the victim of a successful attack. This means that internal changes will be needed – 93% of those surveyed report that there is at least one barrier in their organization when it comes to establishing a better security posture against ransomware.

Clearly, organizations must address cybersecurity awareness issues within their workforce (42%) and a lack of skills in their IT team (40%) through the implementation of a security first approach, including better education, training and/or recruitment procedures.

But the problems will not be solved by improving the workforce alone, it is also critical that organizations augment their security infrastructure so that they have access to more accurate and helpful threat intelligence, which is currently a problem for 37% of respondents' organizations.

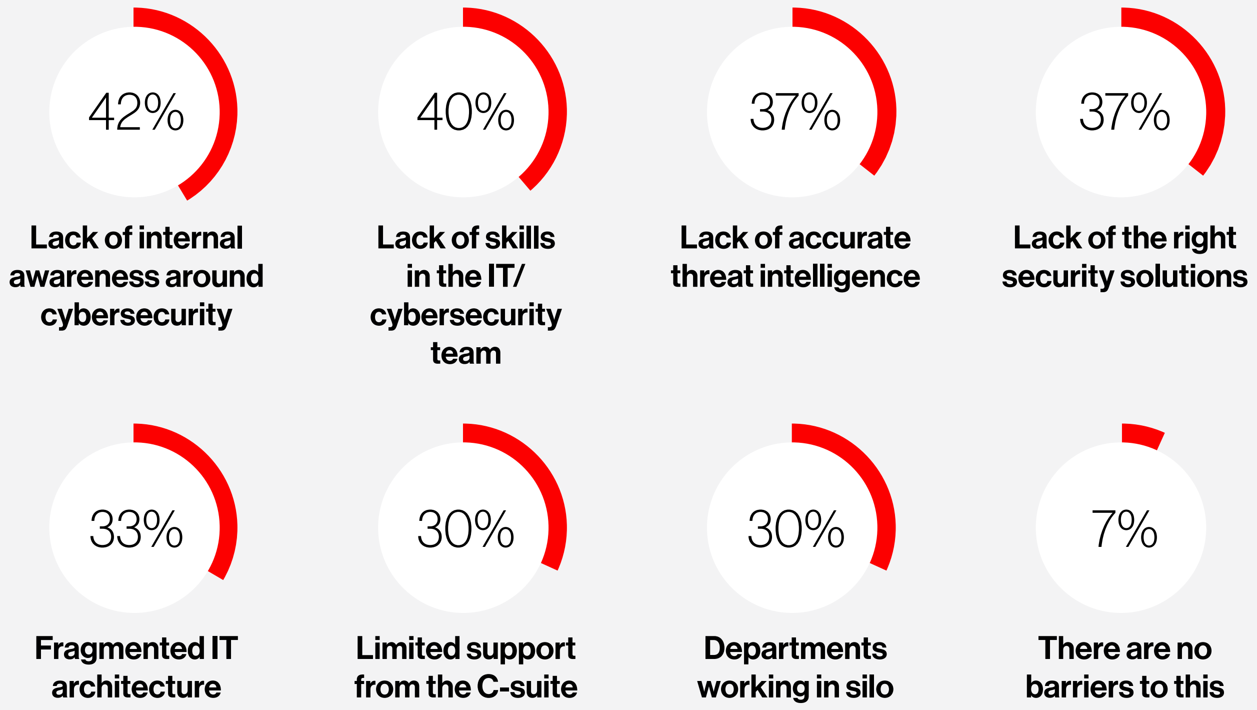

Figure 3: Which of the following barriers exist in your organization when it comes to establishing a better security posture against ransomware attacks? (n = 2,200, omitting some answers)

Ransomware isn't going anywhere, and if anything, it's on the rise. Cybercriminals have had great success when targeting organizations during a period of upheaval over the last couple of years. And while IT teams continue to reinvent the way in which their organization operates, there will likely be ample opportunity for these criminals to continue exploiting any vulnerabilities when using ransomware as their weapon of choice.

This means that businesses around the globe must be extra vigilant in their defense against this threat, and in their response efforts should the worst happen. There are plenty of areas to be addressed internally that could enhance their preventative efforts, while implementing a comprehensive recovery strategy would also be advisable.

Many have paid ransoms in recent times, but with personal consequences for employees, along with financial and reputational ramifications for the organization, it's evident that more needs to be done to limit the damage a ransomware breach can do.

Cybersecurity incident/incursion detection time in hours

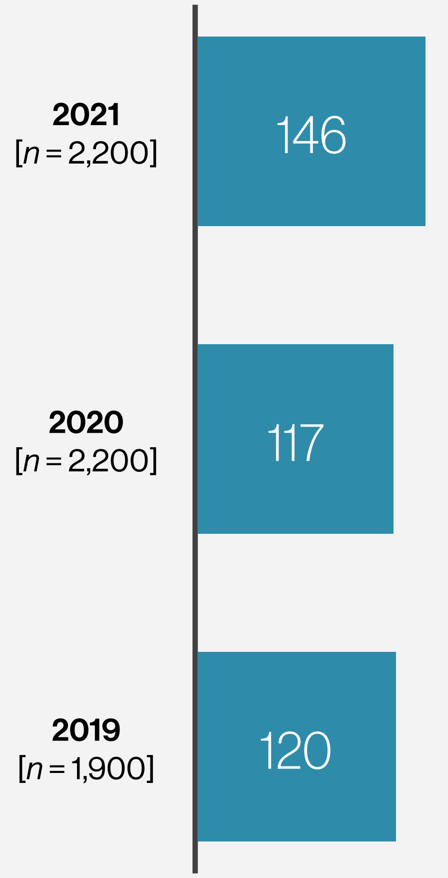

Figure 4: Showing the average time in hours that respondents estimate it would take their organization to detect a cybersecurity incursion/incident

Organizations Are Moving in the Wrong Direction When It Comes to Detection and Response Time

All things considered, being a member of an IT or cybersecurity team over the last couple of years has been an unenviable task. A range of threats – including ransomware and software supply chain attacks – have become more persistent and pervasive than ever, and all the while these teams have been trying to redesign how their entire organization operates from an IT standpoint.

Despite the rising difficulty of defending against these attack vectors, the threat posed by nation-states, cybercriminal gangs, and the mitigating factors imposed by the pandemic, it's clear that organizations must find a way to improve when detecting security incidents as they are unfortunately getting slower. On average, respondents estimate that it would take their organization a staggering 146 hours to detect a cybersecurity incursion, which is a stark increase on the averages reported in 2020 and 2019, which were 117 hours and 120 hours, respectively.

Alarmingly, before many organizations even realize that they have experienced an intrusion, the malicious actor could have been on their network for slightly **over six full days**. In fact, CrowdStrike's ***Falcon OverWatch™ threat hunting team reported*** that eCrime threat actors are able to move laterally across an organization's network in an average of 92 minutes. Recent attacks have shown that many breaches involve more than just malware. Attackers are increasingly attempting to accomplish their objectives without using malware, exploiting the proliferation of vulnerabilities, and abusing systemic weaknesses in identity architecture to get on the system and then moving laterally. This makes it more difficult for legacy and next-generation malware products to be effective because they are not focused on breach prevention. Companies must embrace a holistic, platform approach to security – one that employs both automation and the human element of managed threat hunting – to fight off these pervasive threats.

But, upon detection of the threat there is still plenty of work to be done before the business can once again consider itself secure. According to respondents, it would take their organization an average of 11 hours to triage, investigate and understand a cybersecurity incident, and 16 hours to contain and remediate it. In total this means that, on average, from start to finish there are 174 hours – more than seven days – for the intruder to achieve their objective.

Evidently, this is a far cry from the 1-10-60 paradigm that IT security teams should be striving for.

In an ideal world, this would mean that the incursion is detected in one minute, with 10 minutes allocated to investigating the threat, and then 60 minutes for containing and remediating the issue. There are a range of reasons as to why organizations could be struggling to get close to this model, but if they do not improve their response times, then their data could be gone before they're aware that they have a problem.

One of those mitigating circumstances has unquestionably been the shift to remote working, which has challenged IT teams like never before, and has of course opened organizations up to a range of new risks. Unfortunately, 69% of respondents' organizations have suffered a cybersecurity incident as a direct result of their organizations working remotely. These incidents could have happened for any number of reasons – including human error, which IT teams can only do so much to control – but it does reinforce the need for organizations to address their security flaws if they hope to negate the additional risks posed by remote and hybrid working setups.

However, if there is one positive to come out of the pandemic from an IT point of view, it is that cybersecurity has been brought into the consciousness of a wider range of people. According to 86% of respondents, COVID-19 has been a significant or notable turning point in cybersecurity for this very reason and there is a feeling that people are now beginning to realize the importance of IT security. This can only be a good thing for IT teams, as it should help to reduce the number of incidents that occur due to a lack of awareness from employees around what is expected of them in terms of security best practice.

Nevertheless, there are also areas that are under the direct control of IT teams that are preventing them from responding in a timely fashion when incidents occur. More than nine in ten (92%) respondents cite at least one issue that is preventing their organization from detecting, triaging, investigating, understanding, containing and remediating cybersecurity incursions faster. Chief among these areas, reported by 47% of those surveyed, is that their organization's security infrastructure is made up of too many disparate solutions that don't easily integrate for proper protection and prevention.

While this isn't the only issue holding surveyed organizations back, it does seem to be the most pressing and highlights the fact that an integrated, best-of-breed approach is the way forward. Organizations must untangle the web of tools that they have stitched together over the years, and instead implement a fully integrated solution that can streamline their security infrastructure, thus improving its levels of performance.

Until they have achieved this objective, they will most probably continue to experience long detection times and will be no closer to the 1-10-60 benchmark. This presents far too great an opportunity for cybercriminals to get onto their network, find what they're looking for, and get off again, potentially undetected.

In a world where the prevalence and pervasiveness of a wide range of cyberattacks is only trending in one direction, organizations cannot allow this problem to linger. Acting slowly here will cause them a huge amount of financial and reputational pain, which is not something that they can afford as their recovery from the pandemic continues.

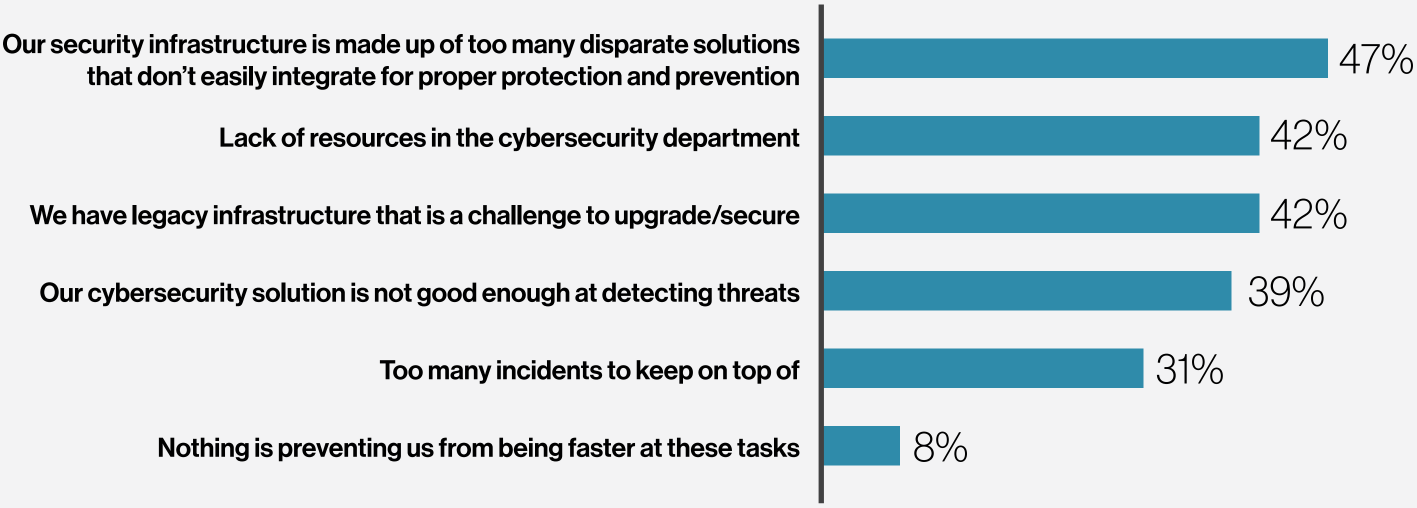

Figure 5: What is preventing your organization from detecting, triaging, investigating, understanding, containing, and remediating cybersecurity incursions/incidents faster? (n = 2,200, some answers omitted)

CrowdStrike Perspective

The insights obtained from security leaders and practitioners on the front lines could not be clearer. The data shows that the threats that organizations are encountering every day continue to accelerate with no sign of letting up. Ransomware continues to be a lucrative avenue for threat actors to monetize their access, made easier by the rapidly evaporating perimeter, enabled by the eCrime ecosystem, driving consistently larger paydays for cybercriminals. No organization is immune; these trends track across industries, geographies and organizational size.

This is the time for defenders to step up their game, but unfortunately that's not happening. We see clearly that the time to detect emerging threats has increased dramatically over the last 12 months. When asked, we see a consistent pattern in the responses. Security organizations are held back by complex technology stacks that are not well integrated, which introduces enormous friction for security teams, while also burying them in mountains of alerts that may hide the true nature of inbound attacks. On top of this, security leaders have lost trust in many of their legacy technology partners, and lack a clear vision for the future.

These trends are on a collision course. Security leaders need to solve for this imbalance if they are going to avoid a damaging breach. CrowdStrike has been focused on tipping these scales for defenders from Day One, and built the CrowdStrike Falcon® platform to address these challenges head on.

The cloud-native ***CrowdStrike Falcon*** platform is fed by a lightweight agent that intelligently collects, enriches and analyzes trillions of events every day, producing actionable insights for security teams. Falcon delivers a foundation for security teams that is simple to deploy, manage and monitor, dramatically reducing alert fatigue. The platform is trusted by thousands of customers worldwide for protecting endpoints from the most sophisticated threats, and extends seamlessly to address cloud security, Zero Trust, XDR and a wide range of plug-and-play partner integrations via the ***CrowdStrike Store***. Additionally, CrowdStrike integrates both managed threat hunting and best-in-class threat intelligence into its security stack. CrowdStrike's Falcon OverWatch team hunts relentlessly to see and stop the stealthiest, most sophisticated threats and helps organizations to make informed decisions to stay ahead of threats. This winning combination empowers security teams to automatically investigate incidents and accelerate alert triage and response. Both are built directly into the Falcon platform, and are able to be deployed and operational within seconds.

CrowdStrike is recognized as a leader by major industry analysts, including Gartner, Forrester and IDC, and is proven in independent third-party testing to be highly effective in stopping today's sophisticated threats.

It's imperative for security leaders to invest in modern security architecture, or risk becoming another cyber statistic. CrowdStrike remains committed to partnering with organizations around the globe to understand the challenges security teams face today, and to delivering trusted solutions needed to stay ahead of the adversary in the future.

Methodology

CrowdStrike commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this white paper is based. A total of 2,200 senior IT decision makers and IT security professionals were interviewed during September, October and November 2021, with representation across the US, EMEA and APAC regions.

All respondents had to be from organizations with 100 or more employees and are from a range of private and public sectors. The interviews were split equally between senior IT decision makers and IT security professionals, and equally between organizations of 100-1,999 employees and 2,000+ employees.

Online and telephone interviews were conducted using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated the results discussed are based on the total sample.

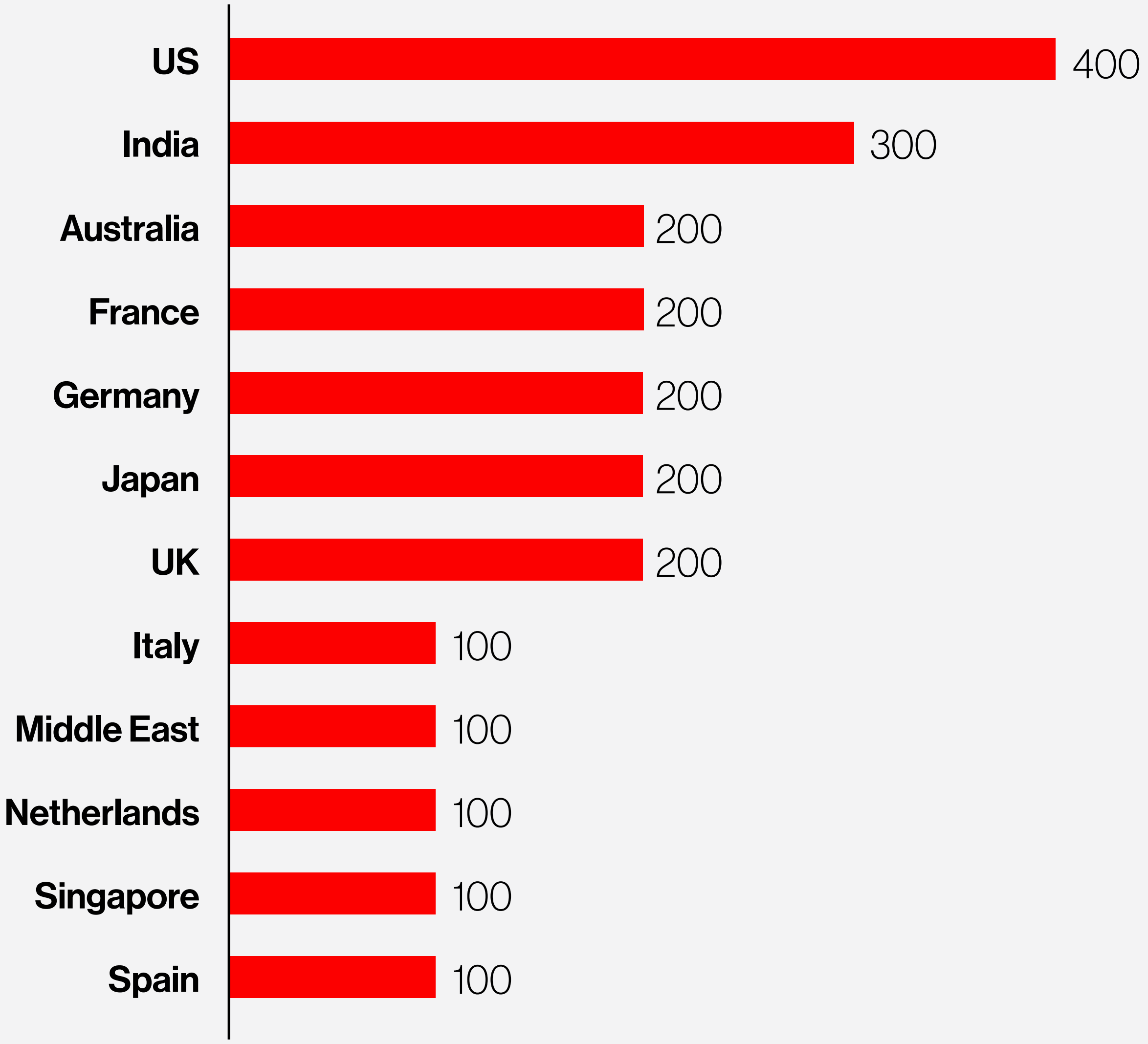

Figure 6: Showing respondent country (n = 2,200)

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon captures trillions of high-fidelity signals per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Qualifying organizations can gain full access to Falcon Prevent™ by starting a free trial.

Learn more: ***https://www.crowdstrike.com/***

Follow us: ***Blog*** | ***Twitter***

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

For more information, visit ***www.vansonbourne.com***