Microsoft

hypothesis

# Security Signals

March 2021

# Table of Contents

# Background

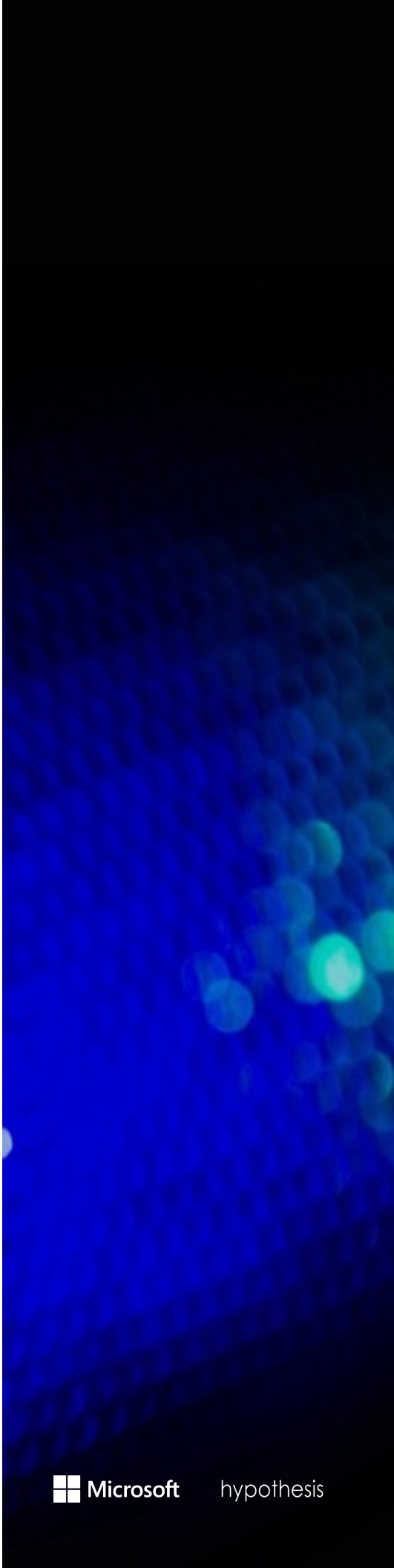
For enterprise organizations, the world of security is a dynamic, constantly evolving space. Looking to protect and secure their organizations, security decision makers are tasked with crafting and implementing strategies that will ensure their companies operate and grow safely.

In a world where security innovations are proliferating--and security threats are growing just as quickly--it is crucial to understand the state of security and the perspectives of those adopting security solutions.

This report sets out to create a detailed picture of the current security landscape: to understand the unique mindset and priorities that security decision makers (SDMs) bring to their organizations; to shed light on the benefits and challenges of adopting security solutions; to assess what impacts and shapes SDMs' business decisions; and to see what the future of security may hold.

The goal of this paper is to provide up-to-date research on the state of security, across countries and industries, in order to better serve our customers and partners, and enable security decision makers to further their development of security strategies within their organizations.

To learn more about the latest insights into the threat intelligence landscape and guidance from Microsoft experts, practitioners, and defenders, check out the Microsoft Digital Defense Report. Informed by trillions of daily security signals, we share our telemetry and insights about the current state of cybersecurity.



# Methodology

Microsoft commissioned Hypothesis Group, an insights, design, and strategy agency, to execute the Security Signals research.

Security Signals Edition One occurred in August 2020, when a 20-minute online survey was conducted with 1,000 decision makers involved in security and threat protection decisions at enterprise companies from a range of industries across the US, UK, Germany, China, and Japan.

In September 2020, a 60-minute online in-depth interview was conducted among six decision makers involved in security and threat protection decisions at enterprise companies from a range of industries within the US.

In addition, an expert panel was commissioned to connect before, during, and after the online survey to identify hypotheses and security trends, as well as validate the research findings.

**This icon highlights quotes from Security Experts throughout the report**

# Things to Know About the State of Security

## Security is fundamental to success, but no silver bullet solution exists

Security is universally seen as critical to organizational success, and SDMs rely on proven industry frameworks to set the strategy. However, the push and pull between preventing against threats and the inevitable need to respond to attacks stretch security teams thin as most of their time goes to table stakes activities like patches and upgrades. Improved efficiency (of both the security team and end users) is the top goal of investing in security, but most organizations struggle with implementing solutions as they debate between a best in breed or best in suite approach.

## Security budgets are expected to be allocated toward more proactive measures

While SDMs are concerned with breaches across software, hardware, and firmware, organizations are component-agnostic when it comes to prioritizing their investments. Today's security budgets are going toward measures that block attackers like firewalls, servers, and advanced threat protection. But organizations know they must take more proactive measures to stay ahead. Two years from now, they plan to invest more in AI/ML, Zero Trust, 5G devices, and TEE to better predict attacks and enable more productivity among their staff. Importantly, those who admittedly experienced a malware attack better understand the impact of a breach and funnel more investment to security overall.

## Automation can free up security teams, but requires continued focus

While increased efficiency is the primary goal of investing in security, and leadership is bought in to investing, security staff still don't spend enough time on strategic work. Consequently, teams are less productive overall and more focused on detection and response than prevention, even though prevention is where they want to be focusing more in the future. Organizations are often stuck in a hamster wheel of recognizing that automation can help free up their resources, but don't have staff knowledgeable in setting up the automation, since automation can involve a total overhaul of security solutions and introduce additional security risk.

# State of Security:
## Overall Research Learnings

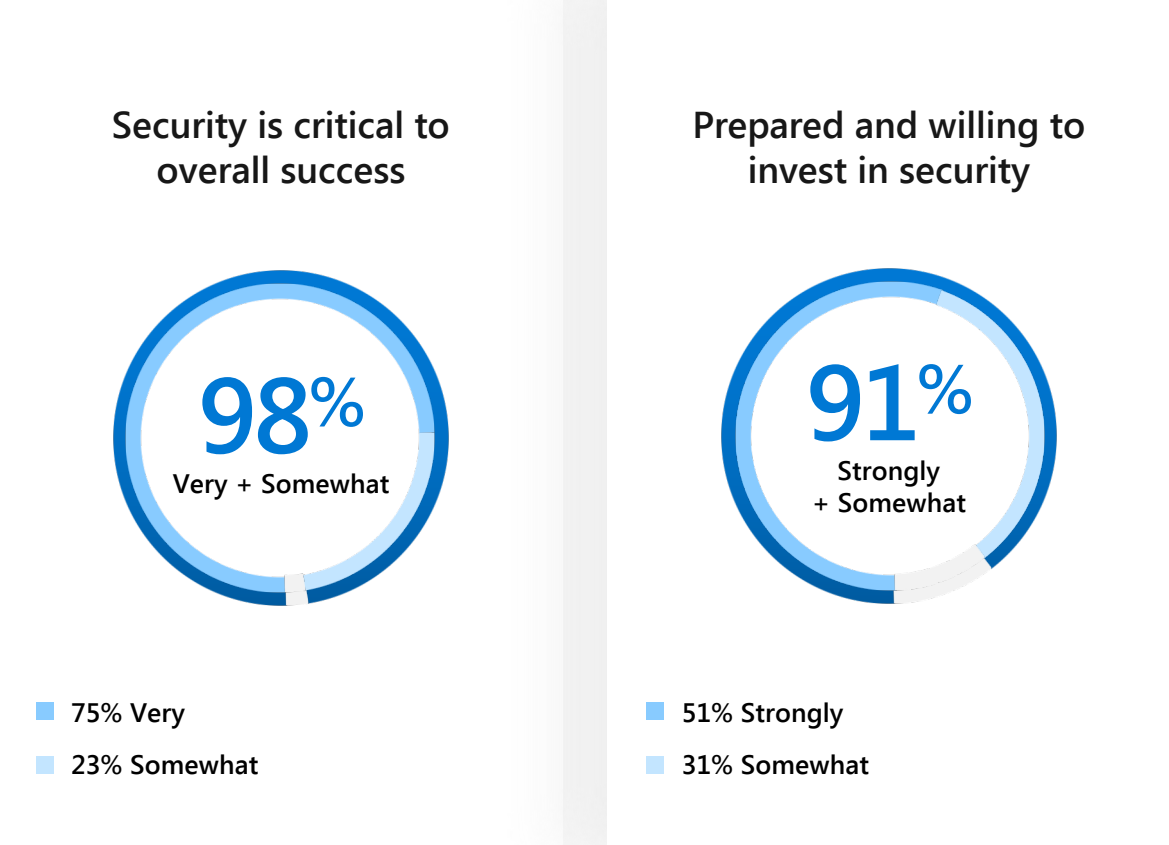
Microsoft hypothesis

# Security: The Big Picture

## Security is foundational to business success

Almost 100% of the decision makers we surveyed believe security is essential to the overall success of their organization. While the majority of decision makers are prepared and willing to invest in security in future (91%), only half feel strongly, suggesting there is plenty of opportunity to help them plan to implement further security measures. **(See Exhibit 1)**

EXHIBIT 1. SECURITY PERCEPTIONS



While most markets and industries have a similar view of security, organizations in Germany and Financial Services are not quite as ready to invest as companies in other industries and markets. 81% of the German companies we surveyed were prepared and willing, as compared to 95% of Chinese organizations and 91% of businesses in the US, UK, and Japan. 88% of financial services companies felt willing and able to invest in security solutions, while 96% of retail businesses were prepared and willing to do the same. **(See Exhibit 2)**

## EXHIBIT 2. SECURITY PERCEPTIONS

| | MARKET | | | | | INDUSTRY TYPE | | INDUSTRY | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | US | UK | Germany | China | Japan | Regulated Industries | Unregulated Industries | Manu-facturing | Retail | Financial Services |
| Security is critical to overall success | 98% | 96% | 97% | 100% | 98% | 96% | 98% | 98% | 100% | 99% |
| Prepared and willing to invest in security | 91% | 91% | 81% | 95% | 91% | 89% | 91% | 93% | 96% | 88% |

Across industries, security decision makers agree that using a proven industry framework lays the foundation for a successful enterprise security strategy. Aligning with a best-in-class framework allows organizations to automate more tasks, measure progress, and follow a solid blueprint as they grow. **(See Exhibit 3)**

## EXHIBIT 3. SECURITY PROFESSIONAL INSIGHTS

### Frameworks lay the groundwork for automation and increased proactivity

*"We can take the NIST framework we use and say, 'if we automate this step, **we've become more proactive** and more secure'."*

Private Education SDM

### Industry frameworks help measure enterprise security progress

*"Adopting and aligning to a best-in-class security framework allows you to **measure and track.** Without a framework, it's difficult to know where to go next and **focus your limited resources.**"*

Restaurant SDM

### A proven framework can be a blueprint as security strategies get more mature

*"We're building programs and capabilities that align to industry standard frameworks to say, 'Here's all the things **as we move up the maturity scale we should be doing to protect** the organization'."*

Insurance SDM

*"Some organizations run their security program based on compliance, but compliance is a metric to see how you are progressing towards a goal, not the end goal. If you work backwards from compliance, you are likely missing pieces. Following a framework can help you start from the bottom up."*

**Robert J. Stratton III, Independent Security Strategy Advisor**

While most markets and industries have a similar view of security, organizations in Germany and Financial Services are not quite as ready to invest as companies in other industries and markets. 81% of the German companies we surveyed were prepared and willing, as compared to 95% of Chinese organizations and 91% of businesses in the US, UK, and Japan. 88% of financial services companies felt willing and able to invest in security solutions, while 96% of retail businesses were prepared and willing to do the same. **(See Exhibit 2)**

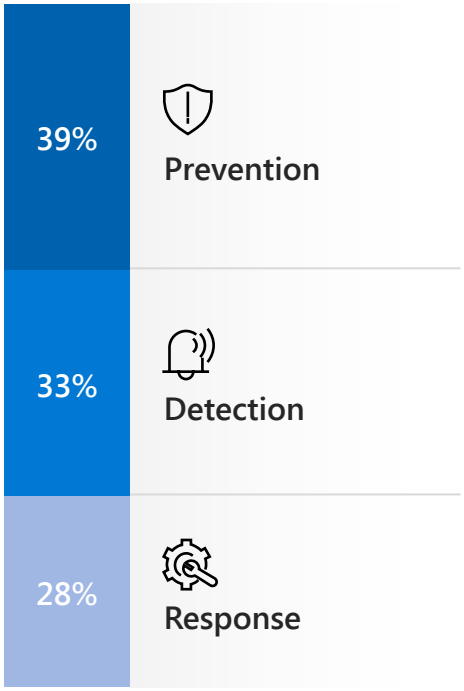
## EXHIBIT 2. SECURITY PERCEPTIONS

| | MARKET | | | | | INDUSTRY TYPE | | INDUSTRY | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | US | UK | Germany | China | Japan | Regulated Industries | Unregulated Industries | Manu-facturing | Retail | Financial Services |
| Security is critical to overall success | 98% | 96% | 97% | 100% | 98% | 96% | 98% | 98% | 100% | 99% |
| Prepared and willing to invest in security | 91% | 91% | 81% | 95% | 91% | 89% | 91% | 93% | 96% | 88% |

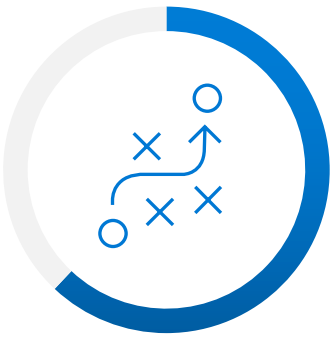
As part of their strategy, security teams are spending almost as much time on detecting (33%) and responding to threats (28%) as they are on preventing (39%). **(See Exhibit 4)** Companies think of prevention in a number of different ways, but all are focused on handling threats through prioritizing which assets to protect, predicting possible targets, educating staff, and adopting preventative tools. They also make sure they're allocating resources to protect their most valuable and vulnerable assets, as well as working to make themselves less of a target for hackers. Since it's unfeasible to prevent all attacks, companies also spend time on detection strategies involving continuous monitoring, automated alerts, and deception traps for possible attackers. Once a threat is identified, the response phase is equally important, focusing particularly on mean time to remediation as a valued metric since disaster recovery can be costly.

While companies' security strategies are clearly important to their business, more than half the decision makers we surveyed said their staff is currently too busy to spend enough time on strategic work. Instead, they are focusing on "table stakes" security issues such as software and firmware patches, hardware upgrades, and internal and external security vulnerabilities. **(See Exhibit 5)**

## EXHIBIT 4. TIME SPENT IN SECURITY TENANTS




## EXHIBIT 5. SECURITY MINDSET



**62%**

**Staff does NOT spend enough time on strategic work**

e.g. setting the security strategy, preparing for sophisticated threats

# Security Benefits

## Investments in security lead to improved efficiency

Companies who invest in security reap a wide array of benefits. Almost two-thirds of SDMs report that security increases efficiency: it frees up security and IT teams to work on other projects, promotes business continuity, and safely enables end user productivity. Almost as many companies say security offers them new and improved capabilities, such as enhanced data availability, confidentiality, and integrity. Other benefits include proactive security, and regulation and compliance. **(See Exhibit 6)**

*"Making the business case for security investment is critical. It shouldn't be considered a cost, but an investment. The money lost due to downtime from a single incident could pay for a solution/headcount to prevent an issue for years. The benefits far outweigh the cost."*

Construction SDM

### EXHIBIT 6. SECURITY BENEFITS

| Efficiency | 65% | New & Improved Capabilities | 61% | Proactive Security | 59% | Regulation/ Compliance | 43% |
|---|---|---|---|---|---|---|---|
| Frees up IT / security team to focus on other priorities | 23% | Enhances confidentiality, availability, and integrity of data | 29% | Protects from imminent threats through cloud-powered updates | 23% | Keeps us compliant with industry regulations | 19% |
| Improves business continuity | 19% | Enhances data management capabilities | 19% | Keeps us ahead of ever-evolving threats | 20% | Protects brand or reputation | 17% |
| Enables end user productivity without sacrificing security | 17% | Secures personal devices for remote work | 17% | Mitigates threats proactively with built-in protections | 20% | Builds consumer trust | 16% |
| Decreases downtime of technology | 14% | Enables our move to the cloud | 13% | Removes the need for outdated systems and technologies | 11% | | |
| Helps save on investments needed elsewhere | 11% | | | | | | |

# Security Challenges

## Security professionals must overcome implementation hurdles

However, security is not without its challenges. 61% of businesses cite difficulties with implementation. In particular, it can be hard to implement security solutions for remote workers, especially as a result of COVID-19. This unique situation left these staff unprepared to protect their environments from security threats while working remotely--this and other resourcing issues were reported by 42% of SDMs as challenges. **(See Exhibit 7)** Another implementation-related challenge revolves around how best to work with vendors. Companies are divided as to whether to take a best-in-suite or best-in-breed approach: 37% want to consolidate how many providers they work with, whereas 43% are looking to enhance their list of vendors.

### EXHIBIT 7. SECURITY CHALLENGES

| Implement-ation | 61% | Resource Constraints | 42% | Ongoing Management | 41% | Cost | 37% | Usage & Breaches | 31% |
|---|---|---|---|---|---|---|---|---|---|
| Difficult to implement security solutions for remote workers as a result of COVID-19 | 18% | Staff unprepared to secure their environment while working remotely as a result of COVID-19 | 16% | Complexity of managing security baselines for all endpoints across multiple OS or versions | 16% | Cost of implementing security technologies | 17% | Enabling end user productivity without sacrificing security | 10% |
| Challenges integrating our security solutions | 15% | Lack of knowledgeable staff to deploy and manage security | 14% | Difficulty in remotely monitoring the health of devices | 12% | Cost of maintaining security technologies | 15% | Returning compromised devices to a secured state | 9% |
| Security projects take too long to implement | 14% | Inadequate internal training & re-training of security policies to prevent negligent behavior among staff | 11% | High volume of threat detection alerts to manage | 10% | Difficult to prove ROI of security investment | 13% | Inability to protect from internal unauthorized access / leaks | 9% |
| Complexity of purchasing / acquiring the right security technologies | 13% | Lack of support from leadership | 8% | Inability to keep up with sophistication of attacks | 9% | | | Inability to protect from external unauthorized access / leaks | 8% |
| Incompatibility with outdated systems | 12% | | | | | | | | |

# Security Threats

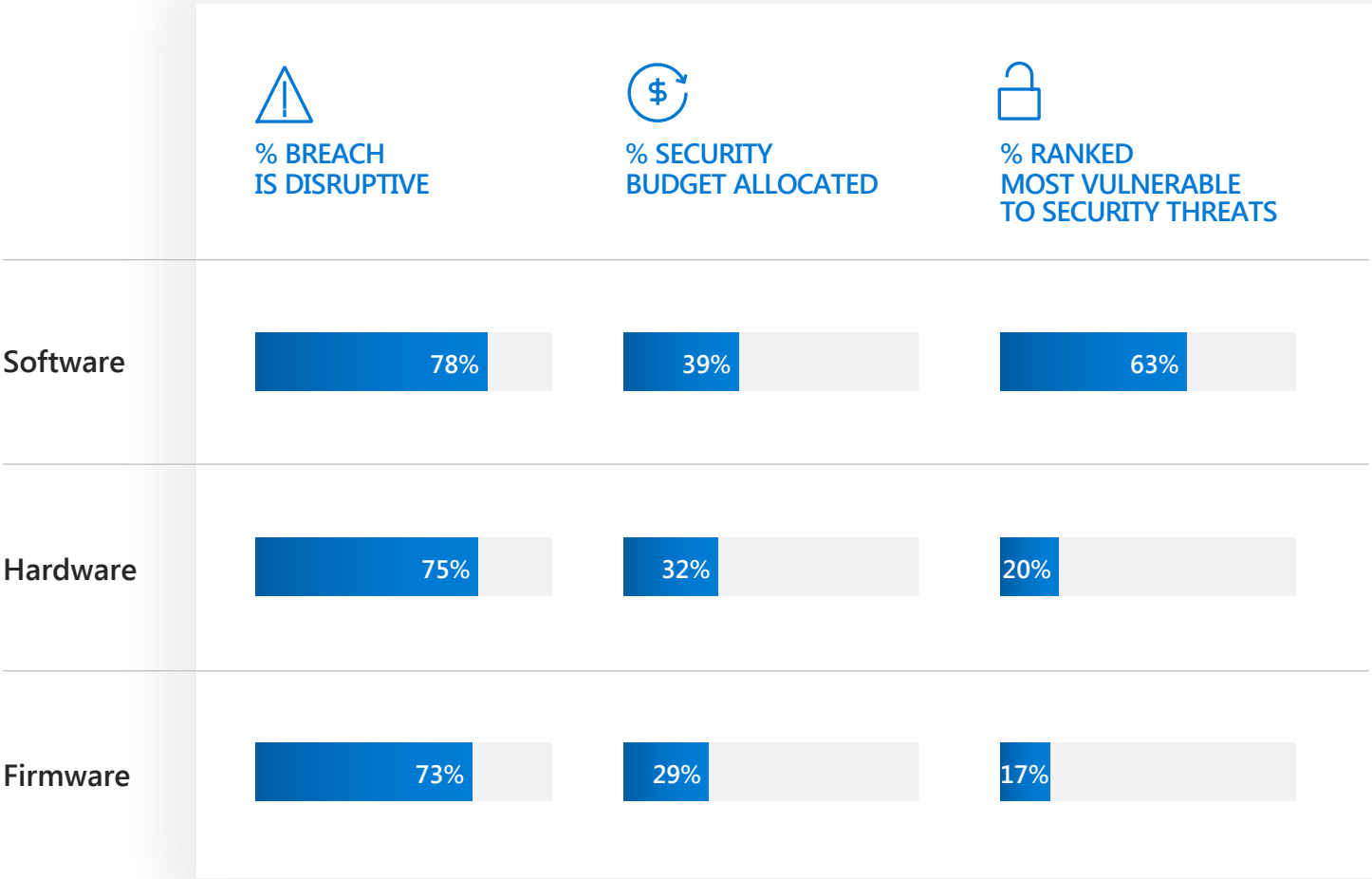
## Security threats are ever-present for all organizations

For the organizations we surveyed, data breaches, unauthorized access, and cyber extortion are top-of-mind security threats. A third of SDMs see data breaches as a top threat, with the US, UK, and China being most concerned. In contrast, companies in Japan have a greater degree of concern about unauthorized access. **(See Exhibit 8)**

EXHIBIT 8. TOP SECURITY THREATS

Most security decision makers, however, see breaches to any security category—software, hardware, or firmware—as disruptive, and allocate their budgets accordingly, spending around a third of their security budget on each category. Software is seen as the most vulnerable to threats, with 63% of organizations ranking it above hardware and firmware. **(See Exhibit 9)**

## EXHIBIT 9. SECURITY CATEGORY PERCEPTIONS



Software, hardware, and firmware threats are perceived similarly across markets and industries; in the US, for example, 63% of organizations view software as most vulnerable, compared to 20% for hardware and 17% for firmware. The exception is Japan, where SDMs consider all three areas almost equally vulnerable. **(See Exhibit 10)**

## EXHIBIT 10. SECURITY CATEGORY PERCEPTIONS

% Ranked most vulnerable to security threats

| | | Software | Hardware | Firmware |
|---|---|---|---|---|
| MARKET | US | 63% | 20% | 17% |
| | UK | 67% | 19% | 15% |
| | Germany | 65% | 19% | 16% |
| | China | 72% | 16% | 12% |
| | Japan | 39% | 31% | 30% |
| INDUSTRY TYPE | Regulated Industries | 64% | 18% | 18% |
| | Unregulated Industries | 62% | 21% | 17% |
| INDUSTRY | Manufacturing | 63% | 19% | 18% |
| | Retail | 66% | 24% | 10% |
| | Financial Services | 71% | 16% | 12% |

# Software

## Organizations invest most in fundamental software protections

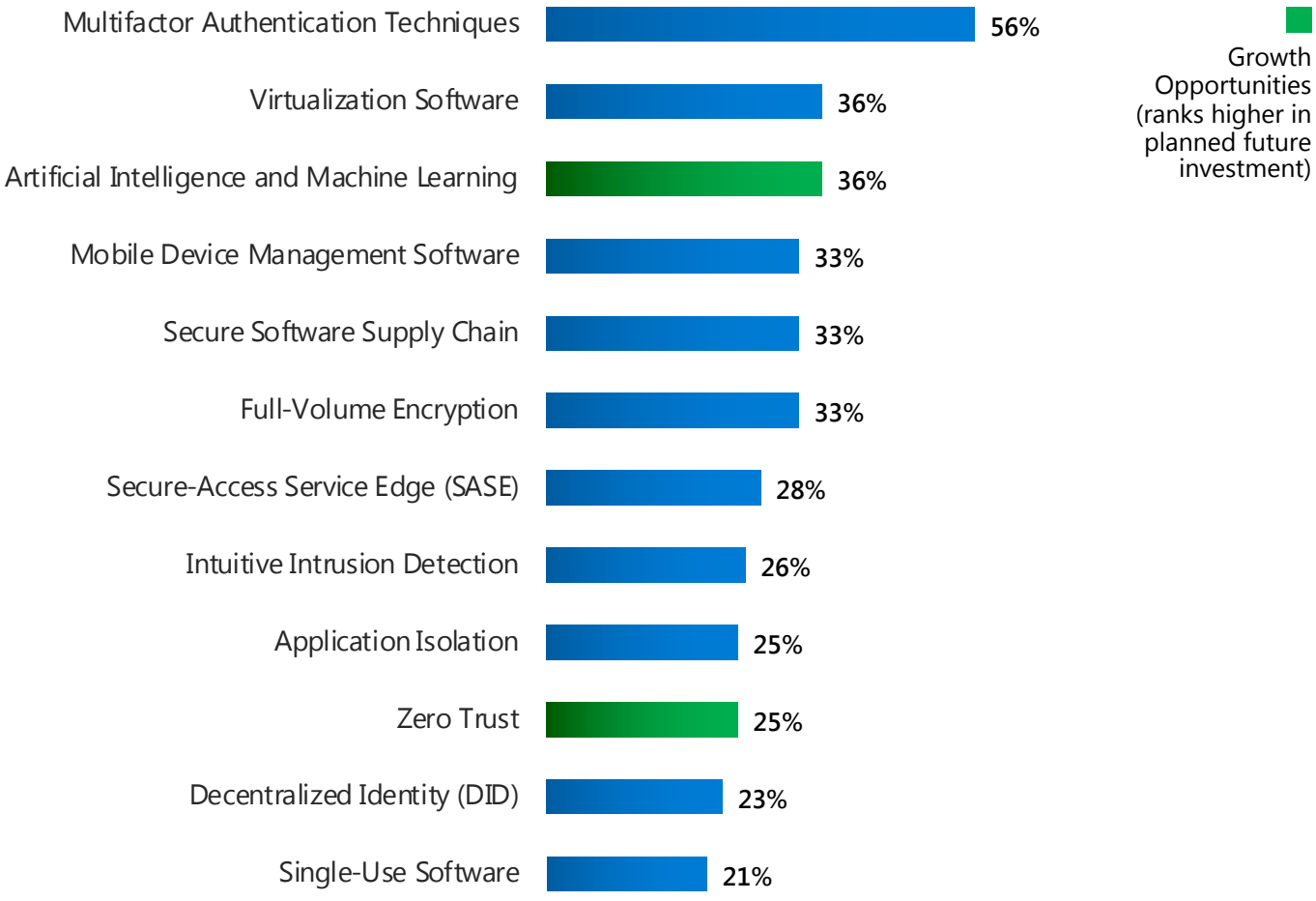
As a result of their concern around software's vulnerability to threats, SDMs are investing heavily in software security. Firewalls are the top investment being made, with 35% of organizations reporting that they are building and using them. Data encryption is also popular, with 32% of companies viewing it as a priority investment. 27% report that they are investing in intrusion detection and prevention. **(See Exhibit 11)**

EXHIBIT 11. TOP SOFTWARE SECURITY INVESTMENTS

| | |
|---|---|
| 35% | Firewalls |
| 32% | Data Encryption |
| 27% | Intrusion Detection and Prevention |
| 23% | Security Information and Event Management (SIEM) |
| 22% | Multi-Factor Authentication (MFA) |

In addition, more than half of organizations are investing in multifactor or password-less authentication techniques, and 36% are investing in virtualization software. AI and machine learning is also a top software project, with a full third of companies investing in the technology. Companies are also planning for future software investments: two years from now, they expect AI and machine learning and zero trust strategies will be even more critical to their company's overall success. **(See Exhibit 12)**

## EXHIBIT 12. CURRENT TRENDS IN SOFTWARE SECURITY INVESTMENTS

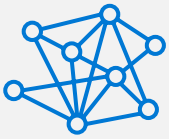


Businesses that currently invest in AI and machine learning (ML) are enjoying benefits such as proactive early warning monitoring systems, automated incident response, and cost efficiency; in the future, AI/ML will help them continue to stay ahead of threats.

Zero Trust will also be key to software security by helping companies take a more proactive approach by assuming hacks can happen both internally and externally. Additionally, Zero Trust helps to enable and secure a remote workforce who may be using their own devices to complete work tasks. **(See Exhibit 13)**

## EXHIBIT 13. SECURITY PROFESSIONAL INSIGHTS

**Azim, Partner at ISG and Former Managing VP at Gartner, says:**



### Looking to the future, organizations should invest in AI/ML even more to stay ahead of threats

*"One of the fastest maturing ideas is applying AI/ML to threat analytics – to different patterns, threat types, etc. These tools are expensive but necessary and worth the investment."*

### Zero Trust will rise in importance as organizations move to a more proactive end-to-end threat management strategy

*"The expectation started to shift that no matter what, you're going to be breached. Companies are starting to realize guarding the perimeter isn't enough. They are adopting Zero Trust to authenticate access at every stop possible."*

# Hardware

## Organizations are moving away from heritage hardware security investments

Most businesses we surveyed consider hardware security critically important, especially companies with more than 10,000 employees. Likewise, bigger organizations are more likely to say that a hardware security breach would be highly disruptive. Companies are investing in larger devices to protect against hardware security breaches: more than half are focusing on servers. Laptops and desktop computers are also key investments for hardware security. **(See Exhibit 14)**

> *"Server investments are high today because they are used as stepping stones in the cloud migration journey."*
>
> **Azim,**
> **Partner at ISG and**
> **Former Managing VP at Gartner**

EXHIBIT 14. TOP HARDWARE SECURITY INVESTMENTS

| | |
|---|---|
| 52% | Servers |
| 49% | Laptops and Desktops |
| 39% | IoT / Connected Devices |
| 29% | Secured Processers |
| 26% | External Storage |

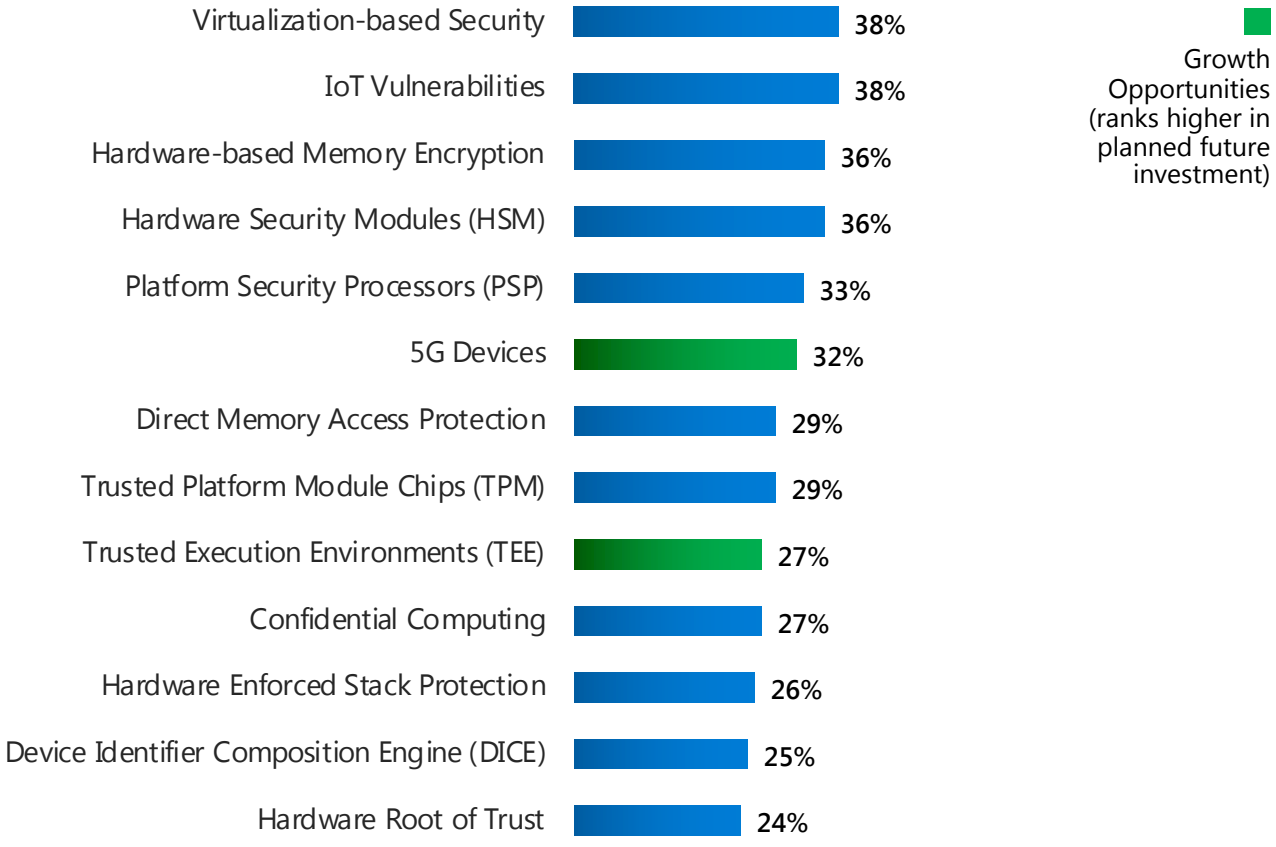
In addition, companies are currently investing in virtualization-based security features and solutions to IoT vulnerabilities, with 38% of organizations focusing on each of these trends. **(See Exhibit 15)** IoT solutions will remain critical to security, since unsecured IoT devices leave organizations vulnerable to threats, and can sometimes react unpredictably to testing.

36% of SDMs also prioritize hardware-based memory encryption as a security solution. Looking toward the future, organizations see themselves investing more in 5G devices and Trusted Execution Environments (TEE). **(See Exhibit 15)**

*"The legacy IoT equipment was apparently designed in the absence of any threat model, except for perhaps those that affected availability risk. So, if you didn't think about the risk, you didn't build anything to protect it."*

**Robert J. Stratton III,**
**Independent Security Strategy Advisor**

## EXHIBIT 15. CURRENT TRENDS IN HARDWARE SECURITY INVESTMENTS

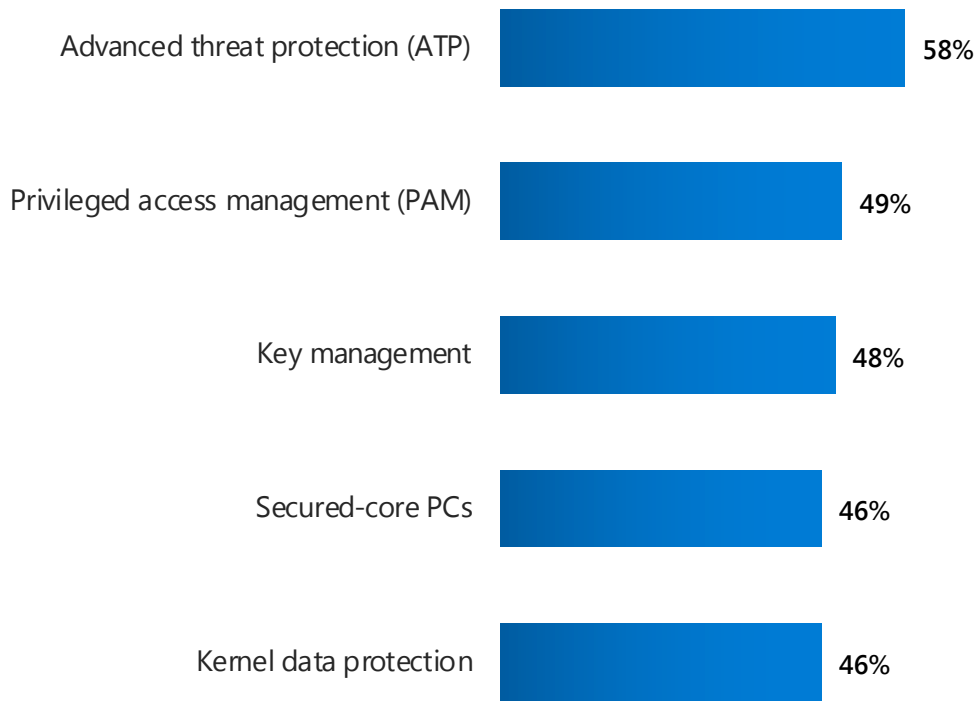


# Firmware

## Mitigating vulnerabilities is critical as firmware security can be difficult to monitor and control

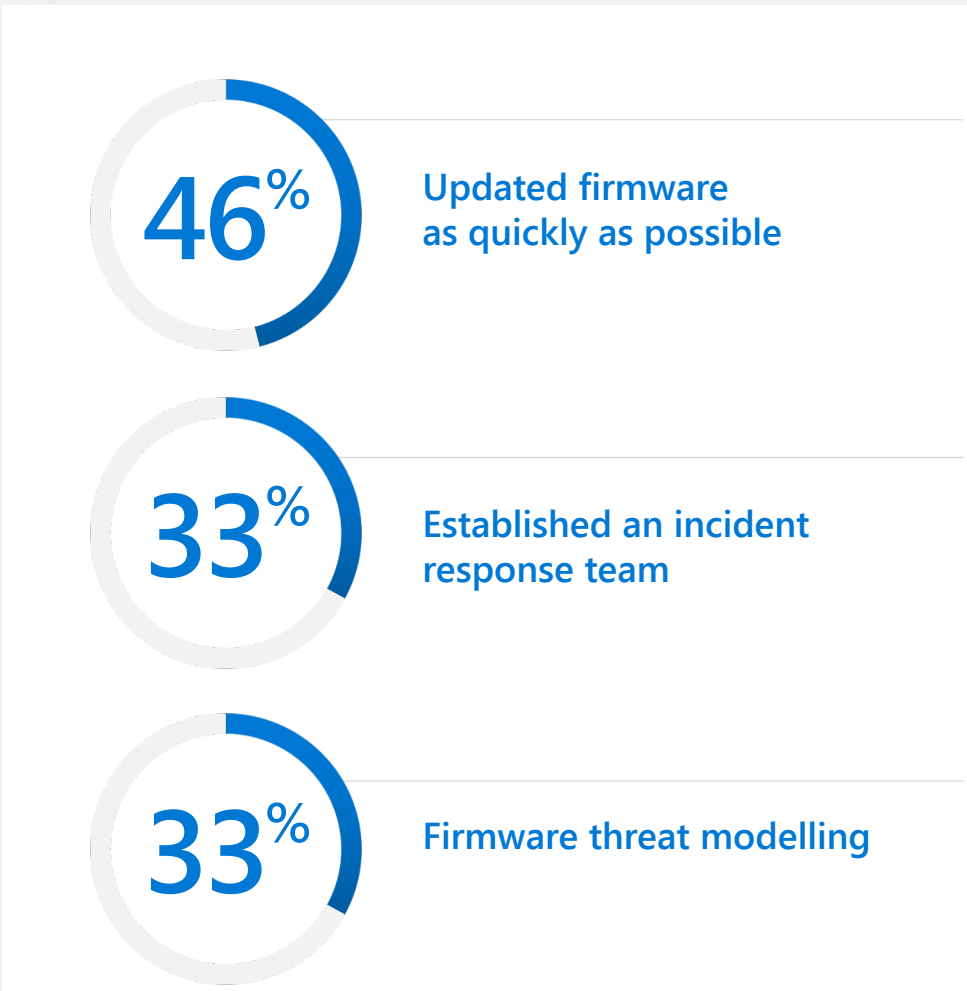
Organizations are currently investing in several firmware security projects. Among the SDMs we surveyed, the top three investments include security updates (26%), vulnerability scans (23%), and security assessment and authentication (22%). Advanced threat protection (ATP) is the top trend organizations are investing in; nearly half invest in other trends including privileged access management (PAM) and key management, along with Secured-core PCs and kernel data protection. **(See Exhibit 16)**

EXHIBIT 16. CURRENT TRENDS IN FIRMWARE SECURITY INVESTMENTS



Despite their investments, SDMs are still concerned about specific firmware threats. Their top concerns are malware gaining full access to systems, the difficulty of detecting firmware threats, the loss of sensitive keys or data, and vulnerabilities introduced in the supply chain. The overwhelming majority of organizations are acting on these concerns: 98% have taken at least one step to manage firmware security. The most common way organizations take this step is to update firmware as quickly as possible. Other top ways that companies protect firmware include establishing an incident response team and modelling firmware threats. **(See Exhibit 17)**

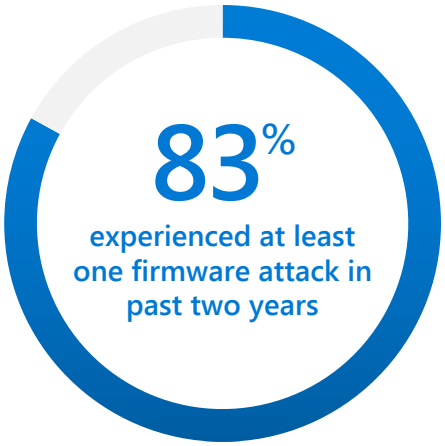
## EXHIBIT 17. TOP PREVENTATIVE FIRMWARE SECURITY ACTIONS



While almost all businesses are taking firmware security seriously, 83% claim they have experienced at least one firmware attack in the past two years—and more companies may also have been vulnerable. **(See Exhibit 18)** Organizations that reported experiencing a firmware attack are more likely to consider hardware and firmware security to be critically important. **(See Exhibit 19)** Relatedly, the organizations who have been attacked spend more of their budgets on firmware security. Conversely, companies who don't report any attacks are investing more in software security. Along with higher overall investment in firmware, those who have been attacked are also investing more in firmware trends: over half are focusing on key management and Secured-core PCs, while 49% are spending on kernel data protection. In addition, these companies are taking more steps to prevent firmware threats. More than a third say they're investing in threat modelling, versus 24% of those who haven't experienced a firmware attack.

> *"There are two types of companies – those who have experienced a breach, and those who have experienced a breach but don't know about it."*
>
> **Azim,**
> **Partner at ISG and**
> **Former Managing VP at Gartner**

## EXHIBIT 18. FIRMWARE ATTACK PROFILE




## EXHIBIT 19. SECURITY PERCEPTIONS (VERY CRITICAL)

| | Organization experienced a firmware attack | Organization has NOT experienced a firmware attack |
|---|---|---|
| Software Security | 69% | 72% |
| Hardware Security | 63% | 57% |
| Firmware Security | 62% | 56% |

# Spotlight on
# **Secured-core PCs**

Microsoft hypothesis

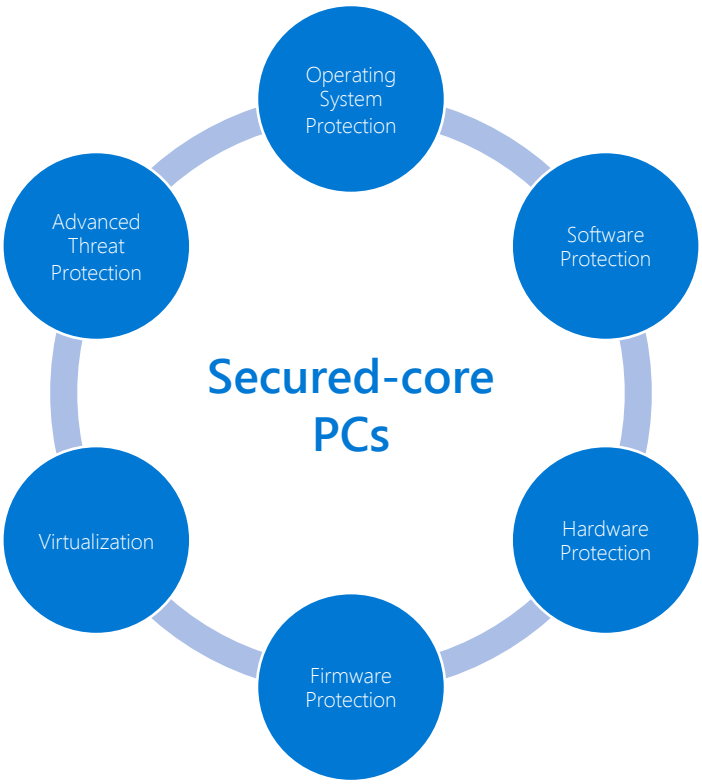
# Secured-core PCs

## Secured-core PCs secure endpoints with chip-to-cloud security allowing SDMs to better safeguard their assets

Announced by Microsoft in late 2019, Secured-core PCs offer state-of-the-art security protection in an out-of-the-box solution. **(See Exhibit 20)** Secured-core PCs mitigate concerns expressed by security decision makers and keeps organizations on the cutting edge by combining hardware, software, and OS protections to provide end-to-end safeguards against sophisticated and emerging threats.

Companies that invest in Secured-Core PCs better understand the disruption breaches can cause. Indeed, among those who invest in Secured-Core PCs, around 80% recognize that a hardware or firmware breach would be highly disruptive to their organization vs. around 70% among those who do not invest.

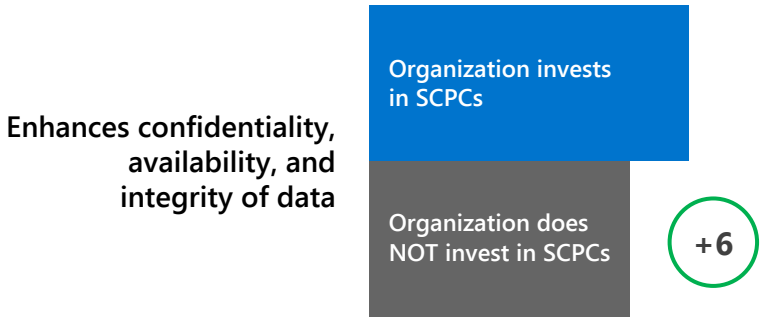
EXHIBIT 20. SECURED-CORE PC SOLUTION



Companies that invest in Secured-core PCs:

- **Demonstrate more understanding that security issues can start at the source**, as 60% of those that invest say that it is important to monitor and have visibility into the OEM supply chain (vs. 49% among those who do not invest).
- **Feel ahead of the security curve**: for example, 87% believe their security strategy is more innovative than industry standards and 85% say they are among the first to adopt new security solutions (as compared to 71% and 74% among those who do not invest).
- **Are alleviated of the need to test and enable these security features**. Perhaps as a result of investing in this new class of devices, SDMs who invest feel a greater sense of overall security as they believe that their data is better protected (32% vs. 26%). **(See Exhibit 21)**

## EXHIBIT 21. SECURITY BENEFITS



# Spotlight on
# **Security Staff Productivity**

Microsoft hypothesis

# Security Staff Productivity

## Automation can free up security staff, but is difficult to achieve

SDMs are reaping significant benefits from their investment in security. Around two-thirds of the companies we surveyed report increased efficiency, including improved productivity both for security teams and end users. 92% of companies say they have support from leadership to invest even more, while 91% believe their organizations are prepared and willing to invest—which is critical to a successful security strategy. **(See Exhibit 22)**

### EXHIBIT 22. SECURITY INVESTMENT MINDSET

**92%**

**have support from leadership to invest more in security**

*"We implement an annual **executive breach scenario** where we bring in a third party to facilitate training with the C level. Attacks are financially motivated, and we know executives are the VIP targets, so training them is a must."*

Restaurant SDM

**91%**

**believe their organization is prepared and willing to invest in security**

*"Leadership will buy whatever we need, we're not worried about funding at all. **We've had competitors go out of business** for not being on top of security. If we can communicate the threat and problem, leadership funds it immediately."*

Finance SDM

> *"If you don't have security ingrained at the top, the effects will ripple down. It doesn't matter how good your employees are or whom you hire. Make it easy for anyone to report a security issue and reward them."*
>
> **Robert J. Stratton III, Independent Security Strategy Advisor**

While productivity has improved, SDMs say it could be better still: 62% feel that their security teams still do not spend enough time on strategic work. Larger companies and unregulated industries struggle more, with around two-thirds reporting suboptimal productivity. **(See Exhibit 23)** However, security teams say they're already operating at or near their maximum capacity.

*"We use analytics to detect and predict, and automation to respond. We have it all now, but it's all DIY, so we can't reduce our staff because we have a hamster wheel of people who need to build the automation. If you had a solution that gave you all the automation, that would help."*

**Insurance SDM**

## EXHIBIT 23. SECURITY MINDEST


*COMPANY SIZE*

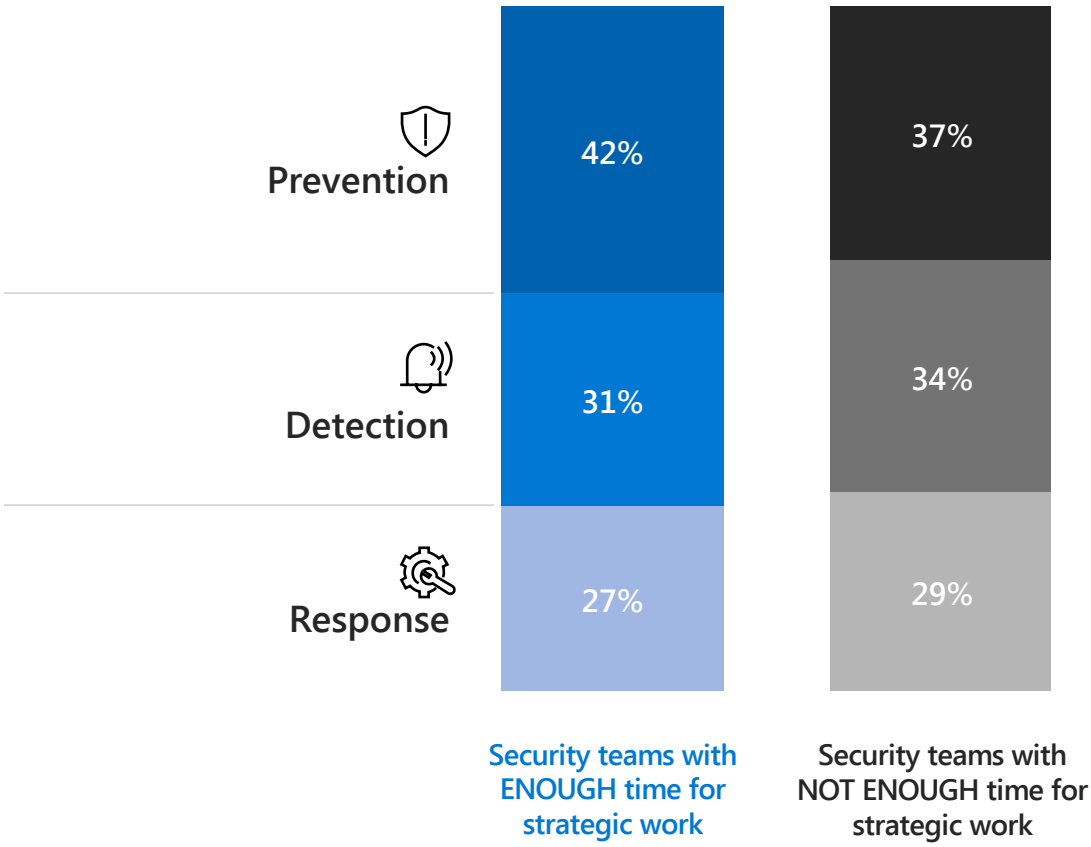
| | |
|---|---|
| 500 – 999 Employees *Non-US Only* | 54% |
| 1,000 – 9,999 Employes | 62% |
| 10,000 or more Employees | 67% |

*INDUSTRY TYPE*

| | |
|---|---|
| Regulated Industries | 55% |
| Unregulated Industries | 64% |

Security teams with enough time to spend on strategic work accomplish more across the board than those who are already at maximum capacity. For example, those with enough time for strategic work spend 42% of their time focused on prevention, whereas those who are at maximum capacity allocate only 37% of their time on prevention. **(See Exhibit 24)** Consequently, preventative measures such as managing security endpoints and penetration testing fall by the wayside for teams with limited time.

## EXHIBIT 24. TIME SPENT IN SECURITY TENANTS



Teams know they can free up time by automating tasks: in fact, almost three-quarters of SDMs say their teams spend too much time on tasks that should be automated. However, SDMs need to acknowledge that increased automation brings risk, as well as potentially requiring more staff than they may have available.

> *"Now that security has gained importance, we see the evolution of the CISO's job from 'the office of no' to understanding and evaluating risk that comes with increased automation. To do a major overhaul of the automation tech footprint often requires more staff than a CISO may have available."*
>
> **Robert J. Stratton III,**
> **Independent Security Strategy Advisor**

# Final Thoughts

Globally and across industries, security is fundamental to organizational success as it enables efficiency, lowers the chances for data to be compromised, and diminishes the potential for more damaging incidents down the line. While most successful strategies tap into proven industry frameworks, organizations are inhibited from investing more in security due to implementation challenges, the complexity of onboarding and managing new solutions, and a lack of resources.

While software is seen as the most vulnerable to security threats, decision makers allocate their security budget equally across software, hardware, and firmware security solutions. Leadership is already bought in and willing to make the investment in security, so the role of decision makers is to find the right solutions that can be seamlessly integrated with existing technologies without overburdening security staff. As a top priority, organizations strive to automate more of their security activities to free up security teams that are already stretched. However, security decision makers must create a bench of staff that is knowledgeable in setting up the automation, as well as acknowledge the increased risk that could be introduced through overhauling the tech footprint.

While most security teams allocate a greater proportion of their time towards prevention, organizations still recognize that threats and breaches are inevitable and consequently allocate an almost-equal amount of time to detection and response. Ultimately, those who align their resources to spend enough time on strategic work have more time to focus on activities across the board, from table stakes maintenance (e.g., firmware patches, software patches) to preventive measures (e.g., penetration testing, managing endpoints).

# Detailed Research Objectives & Audience Recruit

## The objectives of the research included:

1. Understand the unique mindset and priorities that SDMs bring to their organizations
2. Uncover the current landscape, including benefits and challenges of adopting security solutions
3. Assess what impacts and shapes SDMs' business decisions
4. Explore the future of security and how SDMs intend to invest in the future

## To meet the screening criteria, security decision makers needed to be:

A C-Suite, C-1, or C-2 security decision maker at their organization

Employed full-time at an enterprise-level organization (1,000 employees or more; 500+ for non-US markets)

Ages 18+

Involved in decision-making for security and threat protection

## Of the 1,000 security decision makers interviewed for the research wave in August 2020:

In the US and China, 250 security decision makers were interviewed in each country

In the UK, 200 security decision makers were interviewed

In Germany and Japan, 150 security decision makers were interviewed in each country

*Note: Research was conducted during the global COVID-19 pandemic, which was at varying stages of escalation/containment*



Microsoft hypothesis