2021 REPORT

Cybersecurity Trends in Government

A SURVEY OF EVOLVING SECURITY THREATS IN PUBLIC SECTOR

BeyondTrust

TABLE OF CONTENTS

Report Highlights

BeyondTrust commissioned a survey of ***senior federal, state, and local government security professionals*** across the United States, with 200 responses.

(83% in management roles)

Recent government policy actions are galvanizing agency cybersecurity improvements

82%

believe the American Rescue Plan will boost government cybersecurity

34%

assert improvement will be significant

96%

say their cybersecurity budget has adequate funding

Perceived cyberthreats are shifting

TODAY

#1 Risk
Remote worker or contractor vulnerabilities

1-3 YEARS

#1 Risk
Fileless attacks

PAM is ranked a top security control today and will grow in importance with emerging government programs

61%

consider PAM extremely or somewhat important today

71%

of respondents expect PAM to maintain or increase its level of importance within 1-3 years

Cyber fears may have peaked – the future looks brighter

Positive impact of federal initiatives such as the Presidential Executive Order on Improving the Nation's Cybersecurity and the American Rescue Plan

Increase in cybersecurity funding, and the confidence to select the right solutions

A subsiding pandemic that will relieve many IT and security stressors

Introduction

Public sector IT teams are embracing digital transformation and cloud services to support more agile, productive, and cost-effective operations, while better serving constituents.
The pandemic accelerated the work-from-home movement, and now many organizations have recognized the benefits of workplace flexibility and intend to keep it, in some form, as part of their permanent operating model.

While these modernization initiatives have improved productivity, they have also accelerated the demise of the traditional computing perimeter and create considerable challenges for cybersecurity teams. New security risks are being introduced, expanding the attack surface, and creating new planes of privileges and vulnerabilities for adversaries to exploit.

A tsunami of industry-shaking cyberattacks rolling through 2020 and early 2021 starkly exposed how national safety can be imperiled and large parts of society disrupted by breaches and their fallout. Over 250 agencies and organizations were impacted by the SolarWinds supply chain attack alone.

Under increasing pressure to respond to these mounting cyber threats, the White House issued an Executive Order (EO) on Improving the Nation's Cybersecurity, on May 12, 2021. The EO has highlighted the crucial need, and galvanized the push, to rapidly improve national cybersecurity.

Without question, cybersecurity is now a U.S. national security priority.

Public sector organizations bear a special responsibility to protect highly sensitive government and citizen information.

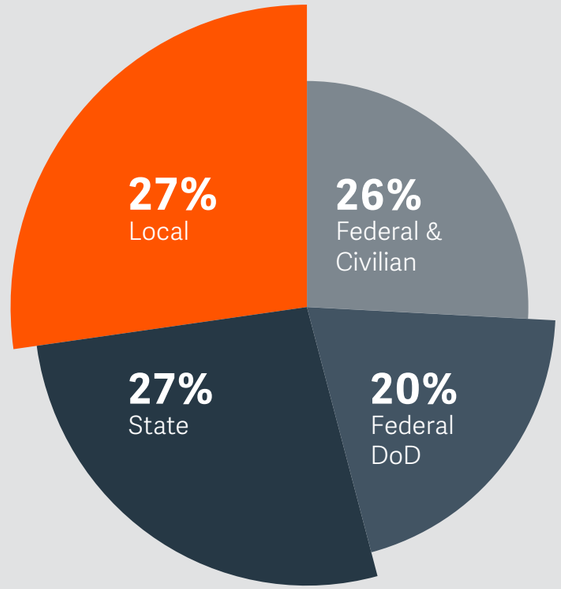
To better understand what keeps public sector professionals up at night, and how they are responding to evolving threats and new mandates, ***BeyondTrust commissioned a survey of senior federal, state, and local security professionals across the United States.***

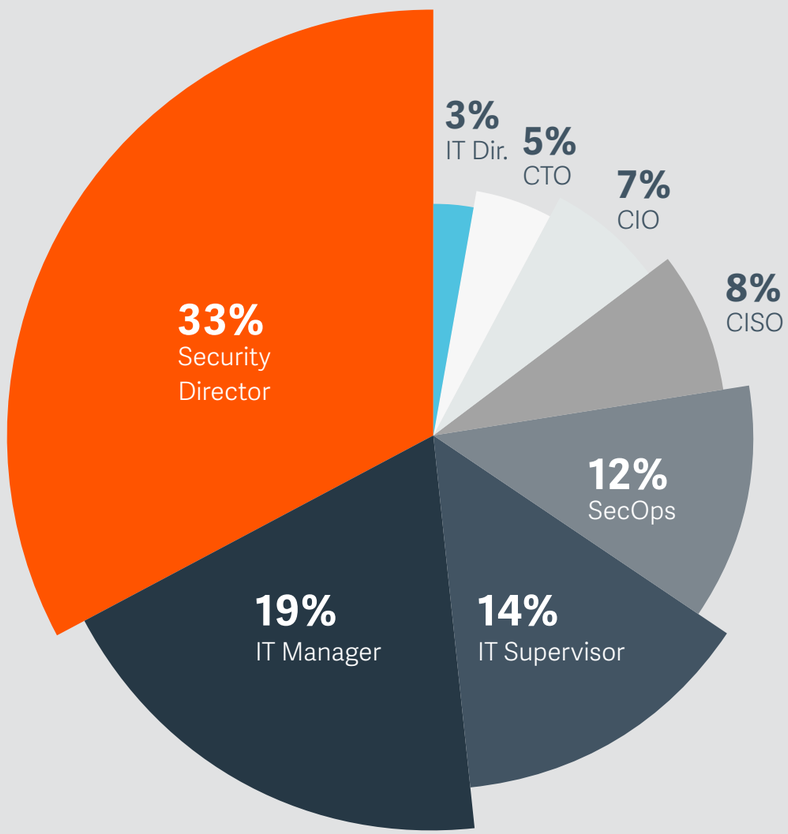
Survey respondents were asked about security trends, concerns, threat actors, and technology priorities—both now and in the future.

Survey Responses

Across senior federal, state, and local security professionals

n = 200





Survey Findings

IT Trends in Public Sector

The survey ranked the level of concern of security trends, both today and in the near future (next 1 - 3 years), and the shifts are intriguing.

Today, ***work-from-home initiatives*** (cited by 54% of respondents), ***cloud adoption*** (38%), and ***increased use of IoT*** (40%) in the public sector each are amongst the most concerning IT trends to our survey participants.

However, looking ahead 1 – 3 years, concern about work-from-home initiatives and cloud adoption both fall by almost half, while concern about IoT also dwindles. These decreases may indicate that IT security leaders feel confident they have identified the measures to better manage these risks.

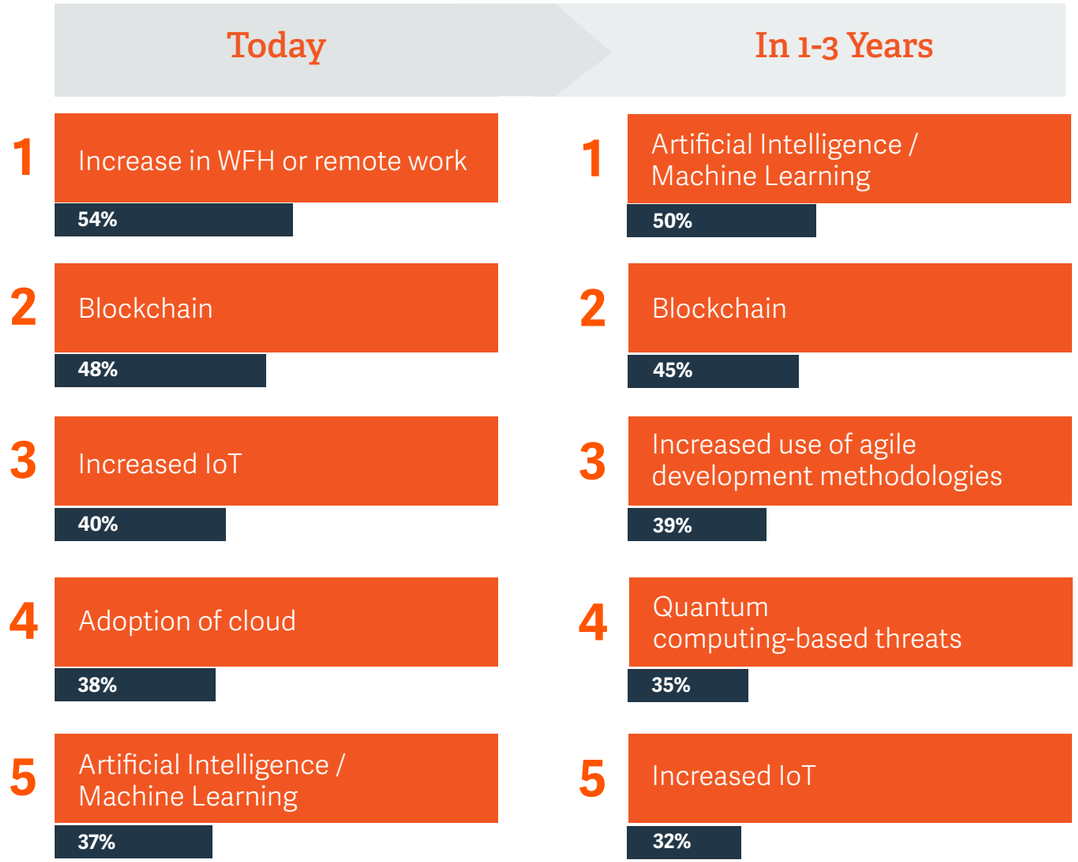
On the other hand, ***artificial intelligence (AI) / machine learning (ML)*** jumps from #5 today (37% of respondents) to the top security concern 1 – 3 years from now, with half of respondents (50%) rating it as a somewhat or extremely high level of future concern.

This shift may reflect the perspective that AI is rapidly coming of age, and organizations lack the tools or know-how to effectively mitigate AI-powered threats.

Threat actors are increasingly incorporating AI/ML capabilities to better weaponize everything from spear phishing to malware that more effectively evades sophisticated detection technologies. Moreover, as public agencies look to wield machine learning technologies themselves, it's important to have the right security controls, implemented correctly, to ensure the technology is not corrupted, misused, or used against them.

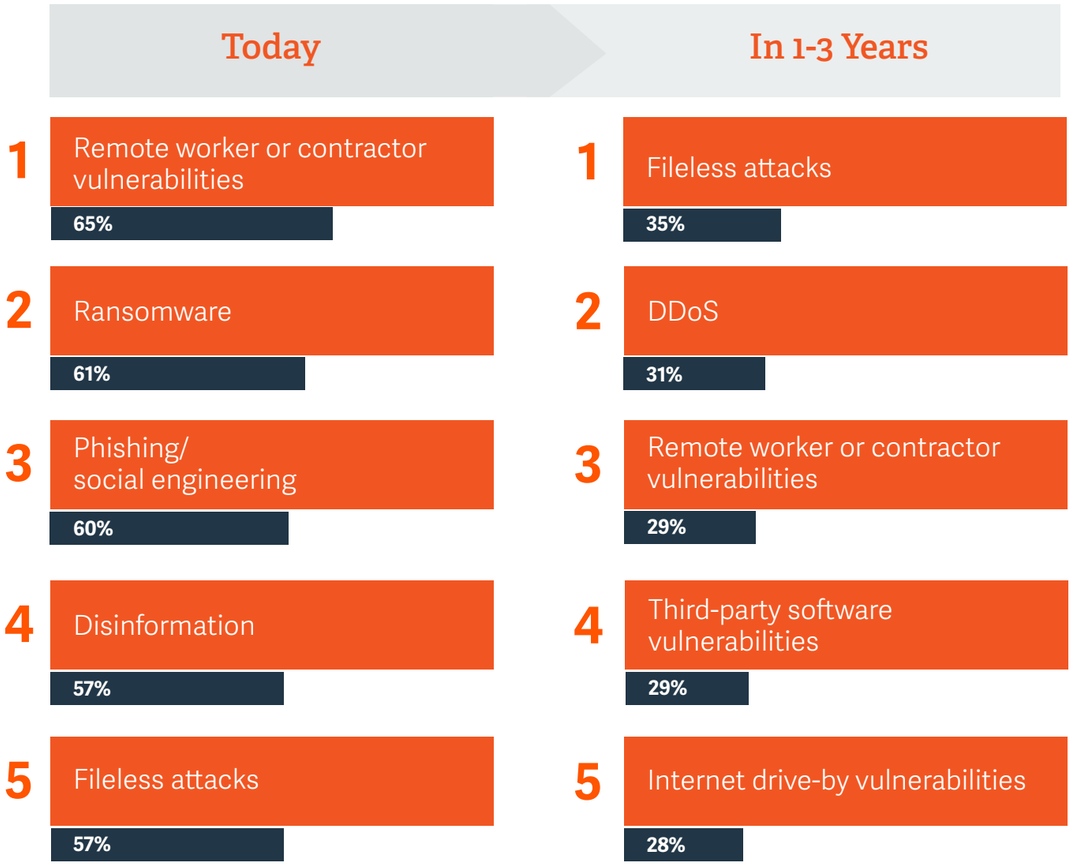
Finally, concerns around ***blockchain*** holds steady at #2 across both time periods surveyed, while ***increased use of agile technologies*** (39%) ***and quantum computing-based threats*** (35%) both landed on the top 5 future concerns list.

Top 5 IT Trends



Over the next three years, the trends concerning security professionals' changes substantially as ***automation, modernization, and digital transformation*** redefine current processes.

Top 5 Cybersecurity Threats



An Evolving Threat Landscape

Survey respondents were asked about the threat landscape, and how they expected it to change over time.

While none of today's Top 5 threats are surprises, it's worth noting that ***disinformation*** may be a more salient concern for the public sector as opposed to the private sector. In recent years, disinformation campaigns have been wielded to threaten the integrity of government agencies, officials, and initiatives, as well as elections.

However, looking ahead 1 -3 years from now, ransomware, phishing/social engineering, and disinformation fall out of the Top 5 and are supplanted by ***distributed denial of service (DDOS)***, ***third-party software vulnerabilities***, and ***Internet drive-by vulnerabilities***.

Notably, fileless attacks leapt from the #5 ranked concern to the #1 concern over the 1-3 year period.

While rankings shifted significantly over time, it's notable that the future concern for every single threat decreased, though it varied by type of threat.

For example, concern for remote worker or contractor vulnerabilities declined by more than half (to 35%), while ransomware concern fell by almost two-thirds (to just 21%).

>>> Overall, public sector security professionals seem confident that they will ***make progress mitigating*** today's biggest threats over the next three years.

Shifts in Threat Actors

Different threat actors have different motives.

While some threats (i.e.; end-user or administrator mistakes) are essentially "motive-less," understanding the different types of attackers can enable organizations to effectively invest in and prioritize the right cyber defenses.

Insider threats have long ranked as a top concern for cybersecurity professionals. The Forrester Predictions 2021 Guide asserts the remote workforce trend will continue to drive a significant increase in insider data breach threats.

Our survey found that insiders are far and away the top cybersecurity concern for public sector infosec leaders today. ***Ill-intentioned insiders*** rank as the #1 concern (67% of respondents), with ***mistakes by insiders*** resulting in security incidents (55%) the #3 highest concern. Concern for ***external threat actors*** (57%) came in at #2, just a little ahead of insider mistakes.

What is fascinating is that, when looking ahead 1 – 3 years from now, cybersecurity professionals indicate much less concern about all insider-related risks, as well as the general category of external threats.

While concern for nation-state actors and organized crime bad actors also decreases when looking ahead, these threat actor categories still rise to the #1 and #2 spots. Overall, ***respondents seem less optimistic about their ability to tackle nation-state actors and organized cybercriminals in the future.*** This is most likely due to the sophistication, and sometimes novel nature, of attacks waged by nation states and organized crime.

In 2021, these attacks were relentless. The SolarWinds breach, attributed to the Russian spy agency SVR, used a routine software update to slip malicious code into Orion's software.

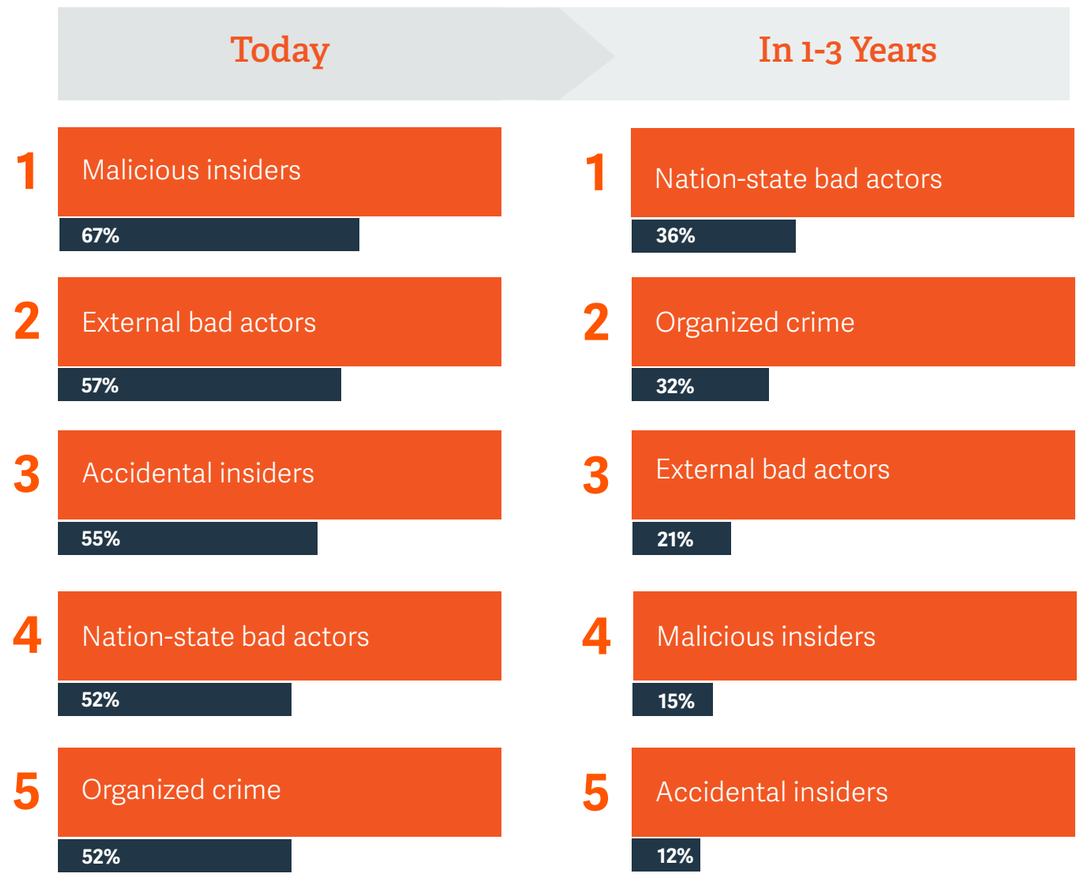
The sophisticated attack went undetected for months and was used as a vehicle for a massive cyberattack that affected thousands of customers. The Colonial Pipeline breach by the cyber-criminal gang DarkSide is another glaring example of nation-state actors taking advantage and targeting critical infrastructure.

The ransomware attack took 45% of the U.S East Coast fuel supply completely offline as Colonial had to shut down its entire network to mitigate the breach.

The re-shuffling in ranking of most concerning threat actors likely reflects the increasing prominence of nation-state attacks initiated by foreign governments such as North Korea, Iran, and Russia.

>>> These entities are often highly resourced, persistent, and motivated, and may target countries and companies with ***attacks like military espionage, or disinformation campaigns*** that can polarize or mislead the public.

Top 5 Threat Actors



Responding to the Threat

MITIGATION STRATEGIES

Now that we have a picture of what cyberthreats are most concerning to the public sector, let's shift our focus to what public sector security professionals are doing to combat cyber threats.

Survey respondents were asked to rate the importance of 21 cybersecurity measures today, and also indicate whether those measures would increase or decrease in importance to them over the next 1-3 years.

Cybersecurity measures were categorized into three groups:

1 BASIC

- Inventory & Control of Hardware Assets
- Maintenance, Monitoring & Analysis of Audit Logs
- Inventory and Control of Software Assets
- Continuous Vulnerability Management
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

2 FOUNDATIONAL

- Data Protection
- Data Recovery Capabilities
- Privileged Access Management
- Secure Configuration for Network Devices
- Secure Remote Access
- Email & Web Browser Protections
- SecDevOps
- Limitation and Control of Network Ports, Protocols, and Services
- Network & Wireless Access Control
- Account Monitoring & Control
- Malware Defenses
- Boundary Defenses

3 ORGANIZATIONAL

- Implement Security Awareness & Training
- Application Software Security
- Penetration Tests & Red Team Exercises
- Incident Response & Management

»»

These categories and security measures roughly mirror those found in The Center for Internet Security (CIS) Top 20 Critical Security Controls.

Note that the CIS recently simplified their list of controls to 18 in version 8.

1 Basic Cybersecurity Measures

Two of the top three most important current measures cited involved the inventorying of assets. ***Inventory of (and control of) hardware assets (74% of respondents) came in at #1,*** with ***inventory and control of software assets (56%) at #3***. Asset discovery and categorization is usually a necessary first step to securing corporate resources and eliminating blind spots that could provide a backdoor for attackers, so it makes sense to see these measures at the top.

In the ***#2 spot is maintenance, monitoring, and analysis of audit logs (63%***), with the majority (53%) expecting it to remain just as important or increase in importance in 1-3 years. Audit trails help organizations comply with government regulations and other mandates. Monitoring and auditing capabilities provide oversight of user activity, helping alert to real-time threats, and also assist with forensics, if needed.

>>> Auditing and monitoring of ***privileged sessions*** is particularly important as those sessions reflect the most sensitive access and most powerful capabilities, with the ***highest damage potential, if misused.***

Continuous vulnerability management sits in the 4th spot, with 52% of respondents rating it as important to them today. For decades, a large percentage of attacks have exploited known vulnerabilities. Prioritizing and patching vulnerabilities remains an effective way to broadly reduce cyber risk and eliminate significant threat vectors, but other measures can help too.

For instance, the Microsoft Vulnerabilities Report 2021 found that ***56% of Critical Microsoft vulnerabilities could be mitigated by removing admin rights***, a very effective method to close the security gaps.

Looking three years ahead, ***53% of respondents expect maintenance, monitoring, and analysis of audit logs to either remain just as important or increase*** in importance, while 55% indicate likewise for continuous vulnerability management. All other basic security measures were overwhelmingly perceived as being significantly less important in the future. Inventory of and control of hardware assets experienced the most significant drop, with 68% saying it would decrease in importance. This decline could be related to the expanded adoption of the cloud, likely due to the continuation of more assets being outsourced and under management of cloud providers or IT service providers.

Ranking the Importance of **Basic** Cybersecurity Measures

1 **GROUP 1**
Basic Cybersecurity Measures

	TODAY *Ranked Somewhat or Extremely Important*	**IN 1-3 YEARS** *Ranked About the Same Importance*	**IN 1-3 YEARS** *Will Become Somewhat or Extremely More Important*
Inventory & control of hardware assets	74%	15%	33%
Maintenance, monitoring & analysis of audit logs	63%	21%	32%
Inventory & control of software assets	56%	12%	17%
Continuous vulnerability management	52%	24%	31%
Secure configuration for hardware and software on mobile devices, laptops, workstations & servers	47%	25%	25%

2 Foundational Cybersecurity Measures

The top 3 measures most often cited as important measures today, ***data protection*** (62%), ***data recovery capabilities*** (62%), and ***privileged access management*** (61%), stand in a virtual tie, while ***secure configuration for network devices*** (58%) and ***secure remote access***, land in the #4 and #5 spots, respectively.

Boundary defense, which encompasses traditional perimeter controls such as firewalls, was rated the least important of the 12 foundational security controls. We imagine that 5 -10 years back, this would have ranked near the top. However, our increasingly perimeterless world characterized by work-from-anywhere, edge computing, and hybrid environments is reducing the effectiveness of boundary defenses.

>>> Of all 12 foundational security controls, ***PAM reported the greatest expected increase in importance*** (40%), and 31% say PAM will remain just as important.

While 71% envisioned privileged access management either staying as important or increasing in importance over the next three years, the #2 spot, data recovery capabilities, trailed far behind, with 56% saying it would stay the same or increase in importance. SecDevOps and data protection followed next, each with 54% of participants citing these measures would increase in importance or stay at the same level. ***The four measures with the strongest future momentum play particularly pivotal roles in protecting against ransomware attacks, while each also address other significant security needs***.

The perceived importance of ***secure remote access***, which has vaulted in priority in the remote work era, is evenly split between those who expect its importance to increase or stay the same versus those who see its importance waning in the next 1 – 3 years. This makes sense as remote working should contract a bit from its pandemic highs. Yet, we expect remote work to remain on an elevated trajectory compared to the pre-pandemic world.

The gulf between the future importance of privileged access management at the top, and the other security controls in the survey only continued to widen down the list. ***Email and web browser protection*** are perceived as having the biggest drop in importance (79%) over the next three years, with the next largest drop seen for ***malware defenses*** (77%), which comprises such technologies as antivirus/antimalware.

Ranking the Importance of **Foundational** Cybersecurity Measures

2

GROUP 2
Foundational Cybersecurity Measures

	TODAY *Ranked Somewhat or Extremely Important*	**IN 1-3 YEARS** *Ranked About the Same Importance*	**IN 1-3 YEARS** *Will Become Somewhat or Extremely More Important*
Data protection	62%	25%	29%
Data recovery capabilities	62%	25%	31%
Privileged Access Management	61%	31%	40%
Secure configuration for network devices	58%	18%	26%
Secure remote access	57%	20%	30%
Email & web browser protections	56%	7%	14%
SecDevOps	56%	17%	37%
Limitation and control of network ports & protocols	53%	21%	25%
Network & wireless access control	53%	19%	34%
Account monitoring & control	52%	24%	27%
Malware defenses	49%	13%	11%
Boundary defenses	41%	23%	27%

3 Organizational Cybersecurity Measures

>>> Within this category, ***implementing security awareness training*** was recognized by 77% of participants as important today.

Awareness training is followed by ***application software security*** (65%), ***penetration tests & red team exercises*** (56%), and ***incident response & management*** (50%).

Since there seems to be a shared acknowledgement amongst analysts and security leaders that experiencing a security incident is practically a given at some point, it's surprising to us that ***incident response & management*** (IRM) was not rated as important by half of respondents.

Lack of mature IRM tools and processes can not only make it challenging to contain a breach, but also much more difficult to recover from a breach. IRM process and tools are also important for providing the breach forensics that may be mandated as part of a breach investigation by government organizations and other regulators, partners, or even courts.

The importance across the four Organizational cybersecurity measures was gauged as remaining fairly stable over the next three years, with none of the radical moves we saw in the other sections.

Slightly more than half of survey respondents saw the importance of penetration tests & red team exercises (53%) and expect security awareness training (52%) as staying as important or increasing in importance over the next three years.

On the other hand, slightly more than half of respondents saw the importance of incident response & management (54%) and application software security (56%) as decreasing in importance.

Ranking the Importance of **Organizational** Cybersecurity Measures

3 **GROUP 3**
Organizational Cybersecurity Measures

	TODAY *Ranked Somewhat or Extremely Important*	**IN 1-3 YEARS** *Ranked About the Same Importance*	**IN 1-3 YEARS** *Will Become Somewhat or Extremely **More** Important*
Implement security awareness & training	77%	13%	24%
Application software security	65%	13%	23%
Penetration tests & Red Team exercises	56%	26%	26%
Incident response & management	50%	36%	24%

Compliance & Government Programs

The 2021 American Rescue Plan is perceived as ***critical for cyber risk management***, with 82% of survey respondents stating the plan will improve cybersecurity, and 34% asserting ***the plan will significantly improve security***.

We also heard from our participants about the importance of various government initiatives today and three years from now, with the most interesting findings featured below.

IT professionals have had a love-hate relationship with compliance initiatives. On one hand, compliance strives to make agency systems more secure, evolve best practices, and uphold agency reputations. Yet the budget, resources and manpower needed to meet these initiatives, on top of regular day to day work, can be daunting.

While 61% say NIST is important to them today versus 18% saying it is unimportant, it's interesting that ***38% of respondents believe the importance of National Institute of Standards and Technology (NIST) policy will increase over the next 1-3 years***. NIST has been an established technology advisor for years and is heavily involved in defining policy within the Presidential Cybersecurity EO.

Another noteworthy finding is that 58% of respondents see StateRAMP as important today and ***40% anticipate it will increase in importance over the next 1-3 years***. StateRAMP is a comprehensive security framework, similar to FedRAMP, designed to improve cloud security for state and local governments. As the move to cloud becomes a common priority across organizations, StateRAMP certainly has reason to catch momentum.

Lastly, ***56% of IT professionals see DHS CISA's Continuous Diagnostics and Mitigation (CDM) program as important to them today***, versus 23% who say it is not. Looking ahead, 35% of participants perceive CDM as growing in importance. The CDM program has been a continued focus for federal agencies by delivering cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture.

Ranking the Importance of **Compliance Mandates**

Compliance Mandates	**TODAY** *Ranked Somewhat or Extremely Important*	**IN 1-3 YEARS** *Ranked About the Same Importance*	**IN 1-3 YEARS** *Will Become Somewhat or Extremely More Important*
NIST	61%	20%	38%
StateRAMP	58%	14%	40%
Section 508/VPAT	58%	23%	29%
CDM	56%	24%	35%
FedRAMP	52%	35%	32%
FIPS	49%	20%	29%
ICAM	47%	25%	25%
CCRI	47%	20%	32%
CMMC	42%	24%	28%

Budget Considerations

As cybersecurity across federal agencies undergoes sharper scrutiny, consensus among the survey respondents seems to be that, at least for now, agencies are armed with the funds and resources they need to address their cyber risk.

In the survey, 56% of respondents said they ***received more cybersecurity budget*** than last year, with 13% receiving significantly more budget. Only 13% of public sector security pros experienced a decrease in their cybersecurity budget, year-over-year.

Along with the American Rescue Plan budget, these funds will also be used to support efforts to share information, standards, and best practices with critical infrastructure partners.

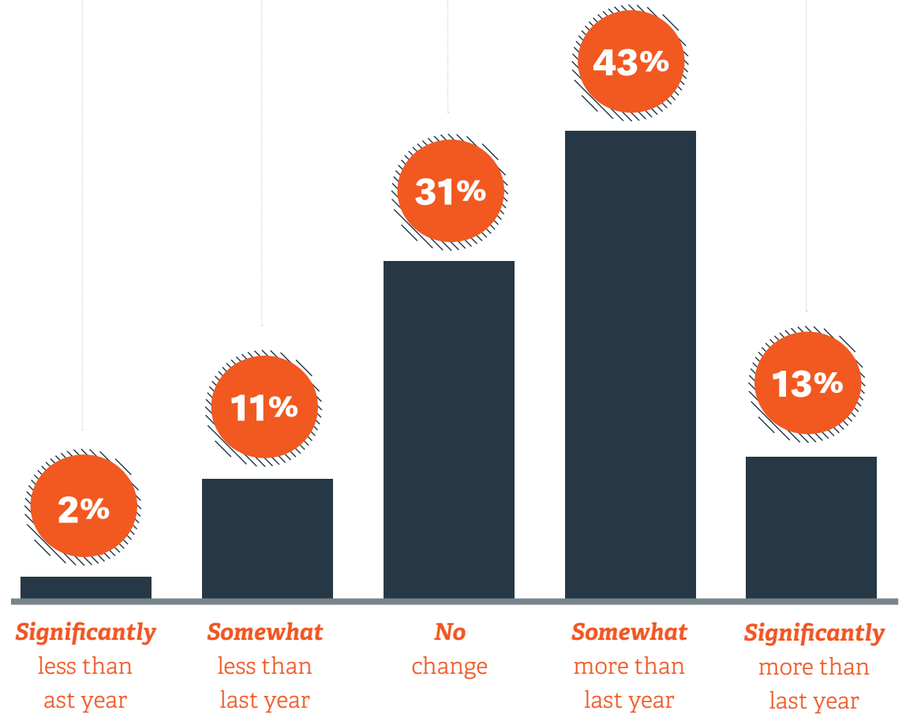
The FY2022 budget requests an additional $500 million for the Technology Modernization Fund, an additional $110 million for the Cybersecurity and Infrastructure Security Agency (CISA), and $750 million to recover from the hacking campaign against SolarWinds.

How do public sector security leaders feel about their level of cybersecurity funding? A miniscule 4% of respondents claimed that their security budget was underfunded.

In fact, an overwhelming ***96% of respondents stated that their cybersecurity budget is adequately funded***.

>>> Biden's 2022 Fiscal Budget requests $9.8B in cybersecurity funding to ***secure federal civilian networks*** and ***protect the nation's infrastructure***, a $1.2B increase from 2021.

How Did Your Cybersecurity Budget Change Year-Over-Year?



Key Findings

Rose-colored glasses, or reasons for genuine optimism?

Government officials have signaled a renewed willingness to aggressively take down cybercriminals – whether run-of the-mill attackers, or nation-state threat actors.

Is this just a case of rose-colored glasses, or is their genuine reason for this optimism?

Our survey reveals ***four potential drivers*** of this positive outlook.

Public sector agencies have undergone a period of massive change that expanded the attack surface, and attackers moved quickly to take advantage. Security leaders are marshalling resources, encouraging collaboration, expanding budgets, and providing updated guidance on best practices to meet these threats.

Though public sector IT security professionals are clearly beleaguered by many security concerns, these leaders project a more optimistic outlook about the threat landscape 1 - 3 years from now.

4 Potential Drivers of Positive Outlook

1 SECURITY TECHNOLOGIES

The Right Security Technologies Have Been Identified and Are Being Implemented

2 TARGETED INITIATIVES

Government Initiatives Are Taking Aim at Attackers

3 BUDGET PRIORITIES

Appropriate Security Budgets Are ***(Finally!)*** Being Funded

4 POST-PANDEMIC

Pandemic-related Stressors Are Subsiding

1 The Right Security Technologies Have Been Identified and Are Being Implemented

Reduced concern about future cyber risks may reflect confidence in the effectiveness of the security measures survey participants are adopting or maturing today, and over the next three years.

At the forefront is ***Privileged Access Management, already ranked as a top security technology today*** by our participants, respondents perceive that it will climb in importance more than any of the other 21 security measures surveyed. PAM solutions manage privileges and blend many other capabilities that are also rated highly in importance by participants, such as secure remote access, maintenance, monitoring, and analysis of audit logs, and DevSecOps.

Other top security measures that participants rated as both highly important today, while also gaining in importance over the next few years include:

- ***DevSecOps***
- ***Continuous vulnerability management***
- ***Data recovery***
- ***Implementing a security training and awareness program***

2 Government Initiatives Are Taking Aim at Attackers

New government policies, like the Presidential Cybersecurity Executive Order (EO) and 2021 American Rescue Plan (ARP), pave a concrete path for cyber improvements and are clearly buoying confidence in the ability to address agency cyber risks. That ***82% of survey respondents indicate the ARP plan will improve cybersecurity (and 34% assert the improvement will be significant)***, demonstrates a strong vote of confidence.

The American Rescue Plan is an ambitious effort to modernize and secure federal IT networks by expanding the Technology Modernization Fund (a $9 billion investment to bolster modernization and cybersecurity efforts). The EO holds agencies accountable to meeting guidelines and timelines to keep pace with the evolving threat landscape. The EO is also helping to define what a zero trust architecture (ZTA) means – helping to move the term zero trust from vision to reality.

Advancing the U.S. government towards zero trust principles is well on its way as OMB and CISA launch a Federal Zero Trust Strategy and a Zero Trust Maturity Model.

3 Appropriate Security Budgets Are (Finally!) Being Funded

With most public sector cybersecurity budgets increasing, and a whopping ***96% of respondents saying their 2021 cybersecurity budgets have been well-funded***, there are valid reasons for wind in the sails of public sector security leaders.

Robust IT security budgets won't solve everything though; correct implementation of technologies may still be hampered by the ongoing difficulty in finding and training new security team members.

However, it is very encouraging that that agencies now have the budget needed to buy and mature high-impact technologies that will address security gaps and improve scalability via automation.

4 Return to "Normal" as the Pandemic Subsides

We believe it's possible that the unique circumstances wrought by the pandemic have created an era of peak cyber risk, and that security adjustments, while lagging, will soon catch up. Three years from now, absent a global pandemic, IT and security teams can simplify their focus and benefit from a return to some measure of day-to-day predictability.

Caveats

While the findings of this report support an optimistic outlook, ***cybersecurity processes and technologies must adapt to what attackers are doing in the future***, not just what is occurring today. The threat landscape evolves continuously, and attackers are always seeking new weaknesses.

Consider the history lesson of ransomware, a threat whose death has been touted by many security leaders and journalists at multiple periods in its 30+ year history, only to emerge re-invented and more dangerous than ever. In addition, survey respondents noted future threat trends (quantum computing, etc.) for which the challenges could become more palpable the closer they come to reality.

Your own environment and its risks are ceaselessly shifting. Don't assume your security posture is strong – constantly test it. Assess the state of your attack surface and vulnerabilities via pentesting, red teaming, and other strategies. ***Unpatched vulnerabilities, default passwords, insecure remote access*** (such as VPNs used for privileged access or RDP exposed to the Internet), ***excessive privileges, orphaned accounts, and misconfigurations*** are just a few common security risks that can give a threat actor that first foothold—or much more.

But most of all,
››› ***stay vigilant & humble.***

Privileged Access Management

A Closer Look

Almost every cyberattack today involves the exploitation of privileges/privileged access—either at the initial point of compromise, or to advance an attack.

Privileged Access Management consists of the cybersecurity strategies and technologies for exerting control over the elevated ("privileged") access and permissions for users, accounts, processes, endpoints, and systems across an IT environment.

PAM solutions aim to manage, secure, and audit every instance of privileged access – whether by human, machine, employee, or vendor.

NIST, CISA, NSA, and OMB, as well as the top industry analysts, have all highlighted Privileged Access Management as one of the most critical cybersecurity areas.

Survey respondents have corroborated their belief that PAM is highly important today, and will increase in importance more than any other of the top security measures over the next three years.

PAM is integral to secure adoption of today's digital transformation and modernization initiatives across the government.

Examples include:

Application Modernization

PAM helps secure your application infrastructure, protecting against both compromise and rogue use of applications across your environment. PAM solutions discover and onboard all application accounts and privileges, while also replacing embedded credentials with API calls or dynamic secrets and enforcing rotation, complexity, and other robust password security requirements. These solutions also lockdown and segment access to applications and harden applications by removing excessive privileges and restricting app-to-app communications. Moreover, granular application control and context-based protections can be applied to further ensure only legitimate, approved applications are used as well as to prevent native process from being leveraged in fileless attacks.

Cloud Adoption

PAM is a foundational technology for securing cloud, multicloud, and hybrid environments, and can address 10 of the top 11 cloud threats ("The Egregious 11") identified by the non-profit Cloud Security Alliance (CSA). PAM solutions continuously discover and onboard cloud and on-premises assets, instances, accounts, etc., and enforce credential security and session monitoring/management best practices—including for control planes. Other important PAM security controls include the enforcement of least privilege, as well as the granular control over applications, commands, files, and scripts to prevent or mitigate errors and malformed/inappropriate commands. The most mature PAM solutions can also enforce segmentation of the cloud environment and proxy remote access to cloud management consoles and compute resources.

DevOps

PAM is an integral part of DevSecOps, and protects tools, identities, and CI/CD workflows, while supporting peak DevOps agility. Some key capabilities of PAM include discovery and onboarding of DevOps assets and accounts, centralized secrets management, enforcement of least privilege, blocking and flagging of inappropriate scripts or commands, prevention of misconfigurations, and the segmentation of development, test, and production systems.

Edge Computing / IoT

PAM solutions can discover, centrally manage (rotate, randomize, enforce strong password security, etc.) for IoT and other devices, and replace embedded credentials with API calls. Fine-grained least privilege and just-in-time access can be enforced across all endpoints and applications. PAM solutions can also secure the remote access connections between edge devices, away from the centralized corporate network, while performing advanced session monitoring that includes, screen recordings, indexing of issued commands, and the ability to automatically identify and stop inappropriate activity.

Robotic process automation (RPA)

Whether you are leveraging attended RPA, unattended RPA, or are leaning into a hybrid approach, PAM protects your software robot identities, RPA workflows, and all the data involved. PAM solutions continuously discover and onboard RPA assets, enforce credential and session management best practices, and enforce least privilege across processes, toolsets, and workflows.

Zero Trust

According to a recent IDSA study, 93% of IT security pros say zero trust is strategic to securing their organization, with 97% asserting identity is a foundational component of a zero trust security model. PAM is a necessary component for enabling zero trust environments and architectures and can enforce context-based least privilege in alignment with just-in-time access models - meaning that privilege is limited both in scope and duration. PAM can enforce segmentation and microsegmentation to further limit lateral movement and line-of-sight to corporate resources. Every privileged session is monitored, managed, and audited – whether human, machine, employee, vendor, remote, or on-premises.

Today, agencies are leveraging Privileged Access Management to boost cyber immunity to:

- ***Malware and ransomware***
- ***Insider threats – both intentional actions and unintentional (i.e. mistakes)***
- ***External threat actors (cybercriminals, nation-state actors, etc.)***
- ***Fileless threats***
- ***Remote access risks***

>>> Increasingly, PAM controls are also required by cyber insurers to obtain coverage and get the best rates.

The BeyondTrust PAM Solution

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides ***visibility and control over the entire universe of privileges*** — identities, endpoints, and sessions. BeyondTrust delivers what industry experts consider to be the complete spectrum of Privileged Access Management solutions.

BeyondTrust is named a ***Leader in the Gartner Magic Quadrant,*** as well as a ***'Gold' Winner of the 2020 'ASTORS' Homeland Security Awards.***

The BeyondTrust Solution

ON-PREMISES | CLOUD | HYBRID

PRIVILEGED PASSWORD MANAGEMENT

Discover, manage, audit, and monitor privileged accounts and sessions of all types

SECURE REMOTE ACCESS

Secure, manage, and audit remote privileged access sessions for vendors, admins and the service desk

ENDPOINT PRIVILEGE MANAGEMENT

Remove excessive end user privileges on Windows, Mac, Unix, Linux and network devices

CLOUD PRIVILEGE PROTECTION

Discover, visualize, and manage entitlements across your multi-cloud infrastructure

BEYONDINSIGHT DISCOVERY | REPORTING | THREAT ANALYTICS | CONNECTORS | CENTRAL POLICY & MANAGEMENT

Protect against threats, achieve compliance and support your mission with BeyondTrust.

BeyondTrust PAM provides powerful, blended threat protection.
Public sector organizations are leveraging BeyondTrust solutions to:

Discover, inventory, and categorize all assets and accounts to bring them under management, while also eliminating blind spots and illuminating shadow IT.

Onboard and manage all privileged credentials and secrets (human and non-human) to protect against password re-use attacks and prevent privileged account compromise.

Enforce least-privilege across users, applications, endpoints, etc. to drastically reduce the attack surface and minimize lateral access pathways.

Provide secure remote access for employees, vendors, and service desks – without VPNs – while also enabling agencies to lock down access to cloud, virtual and DevOps control planes and other consoles.

Apply just-in-time access models to ensure elevated access is only given for a finite period of time and is immediately revoked after the activity is performed, the context has changed, or a certain amount of time has elapsed.

Prevent execution of errant or inappropriate commands, and alert on such instances.

Granularly control applications and employ Trusted Application Protection to thwart fileless threats.

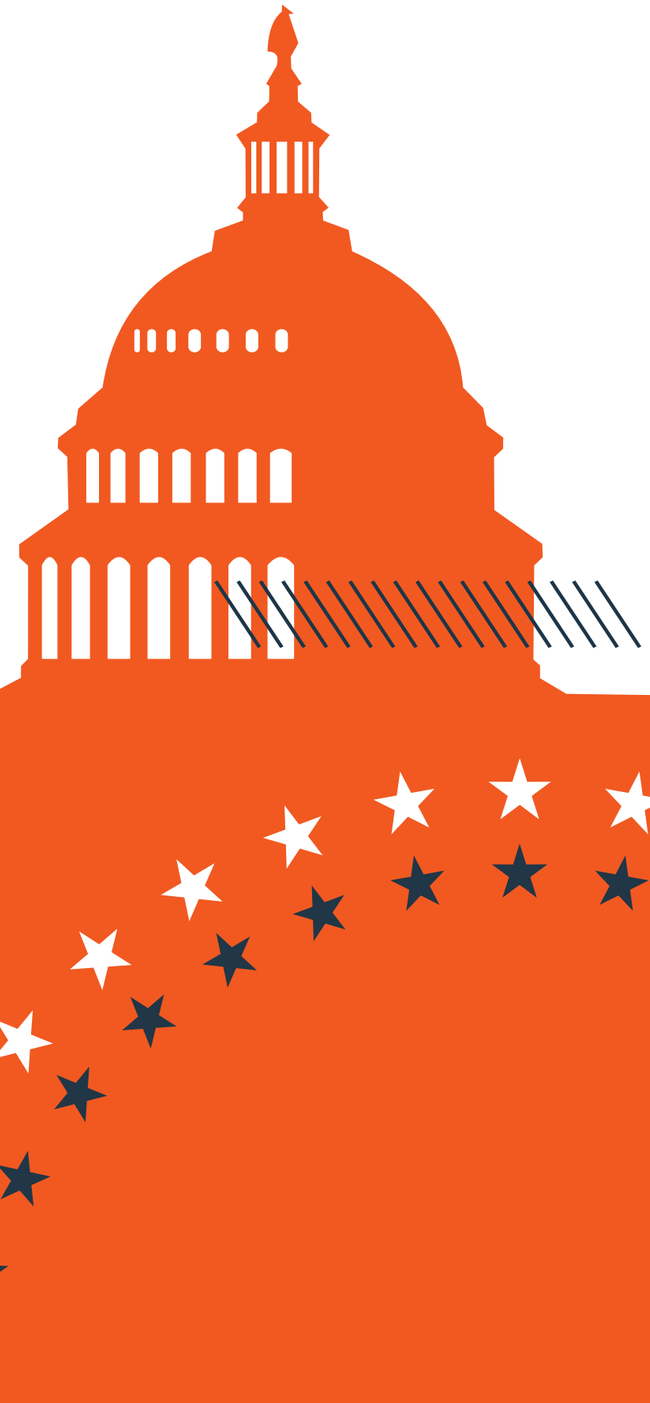
Monitor, manage, and analyze every privileged session, while also providing an unimpeachable audit trail, and the ability to pause or terminate suspicious sessions.

For More Information

Visit our website at **www.beyondtrust.com/solutions/public-sector.**

Additonal Resources

SOLUTION BRIEF	The Executive Order on Improving the Nation's Cybersecurity
WHITEPAPER	Mapping BeyondTrust to CIS Controls 7.1
RESEARCH REPORT	Malware Threat Report 2021
WHITE PAPER	The Guide to Multicloud Privilege Management
SOLUTION PAGE	How BeyondTrust Secures & Enables Digital Transformation
SOLUTION PAGE	Achieve Zero Trust with BeyondTrust



BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust provides solutions that are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

beyondtrust.com

V2021_10_ENG