



2022 CYBERSECURITY SURVIVAL GUIDE

Recalibrate your Security
for Today's Threats



TABLE OF CONTENTS

Executive Summary: The State of Cybersecurity	3
The Path of Least Resistance is Shifting	5
Accelerated Digital Transformation	5
A Multicloud World, with Multicloud Challenges	7
Growth of Unsecure Remote Access	8
Increase of Vulnerabilities Everywhere	11
The Explosion of Unmanaged Privileged Identities, Access, and Sessions	12
The Interconnectedness of Everything	14
Shifting Physical Security Threat	16
Threat Vectors Heating Up	17
Phishing Attacks Are Surging	17
Fileless Attacks are Rising	18
Ransomware is Winning	20
How To Tip the Scales Back on Cyber Attackers	22
Survival Strategy 1: Protect Privileged Identities	25
Survival Strategy 2: Secure Remote Access	30
Survival Strategy 3: Apply Endpoint Privilege Management	33
Survival Strategy 4: Apply Hardening and Vulnerability Management	37
Survival Strategy 5: Prevent Tampering of Mobile and Remote Endpoints	39
Survival Strategy 6: Secure and Empower the Service Desk	42
Survival Strategy 7: Perform Remote Worker Penetration Testing, Carefully	44
Recalibrate your Security with BeyondTrust	49
Additional Resources	52



EXECUTIVE SUMMARY

The State of Cybersecurity

Many of the workplace changes accelerated by the pandemic are expected to endure, and a more durable hybrid work environment is taking root.

The 'New Normal' is here.

The Wall Street Journal called the hybrid workplace a “Cybersecurity Nightmare,” and characterized it as “a hacker’s dream—a constantly changing mix of office and remote workers, devices that move in and out of the company networks, and security staffs stretched thin.” The Wall Street Journal also briefly called out how organizations gain control over this environment – with strong identity-centric security and zero trust.¹



THIS GUIDE INCLUDES:

- 1 Research-backed data and anecdotes illustrating how the attack surface is changing
- 2 Analysis of how the threat actor’s path of least resistance is shifting
- 3 A dissection of several world-shaking breaches over the past year and how they could have been dismantled at multiple steps
- 4 Survival tips that will enable you to adapt, close security gaps, and reduce risk—all while achieving business benefits from the opportunities presented by the new normal

Read on to understand the shifting threatscape and the security strategies and technologies you can put in place to mitigate the risks, while positioning your organization to safely reap the benefits of digital transformation (DX) and remote working.

1- Rundle, James. (2021, June 8).

Why the Hybrid Workplace Is a Cybersecurity Nightmare. The Wall Street Journal.



What is the “New Normal?”

Data protection is a moving target in the work-from-anywhere (WFA) era. As the attacker’s path of least resistance (POLR) to corporate data and assets is shifting, so too must IT risk management priorities. [Antivirus software \(AV\) misses 60% of attacks](#), and many IoT (internet of things) and OT (operational technology) devices cannot even install AV. Firewalls are frequently circumvented, or irrelevant, in distributed computing environments, especially in a multicloud world.

Many organizations have purchased cyber liability insurance to help protect against the financial costs of cyberattacks. However, the blistering pace and expanding scope of cyberthreats and ransomware attacks are prompting cyber insurance companies to steeply increase their premiums, mandate certain security controls and proof of security maturity from their customers, and even drop coverage for high-risk organizations and specific vertical markets. Some cyber insurance providers are exiting the industry altogether, leaving the market short on suppliers who are willing to underwrite policies.

We have clearly entered an era of “assume breach” and “zero trust”. Therefore, we need to not only rethink security, but to also recalibrate it based on the changes to technology that are happening around us.





The Path of Least Resistance is Shifting

Let's explore a few more key trends that are shaping the modern threat environment.

Accelerated Digital Transformation

According to a [McKinsey Study](#), organizations responded to the COVID-19 pandemic by accelerating digitization of their customer and supply-chain interactions and of their internal operations by 3-4 years. McKinsey also found that the share of digital or digitally-enabled products within an organizations' portfolio accelerated by a remarkable 7 years!



➤ “Digital adoption has taken a quantum leap at both the organizational and industry levels. Along with the multiyear acceleration of digital, the crisis has brought about a sea change in executive mindsets on the role of technology in business.”

- McKinsey & Co Survey





Yet, while digital transformation has experienced an evolutionary quantum leap, so too has the cyber threat landscape. The problem is that cybersecurity controls and strategies have not experienced a commensurate leap in their maturity, and consequently, they lag behind modern threats.

Security exposures, compliance gaps, and vulnerabilities are proliferating. Without question, this is playing a pivotal role in the staggering scope and volume of cybersecurity incidents and breaches since late 2020.

SolarWinds, Verkada, Colonial Pipeline, JBS, Kaseya, and a continued scourge of devastating ransomware attacks, are recent examples of threats imperiling supply chains and impacting the daily lives of many millions of people.

While the rapid acceleration of digital transformation has helped organizations innovate, unlock efficiencies, and enable more remote work, it's also tipped the scales of the perpetual cyber arms race decidedly in favor of criminals.

Today, remote workers are frequently operating from insecure Wifi or personal devices. Many users have self-provisioned various apps - often referred to as "shadow IT" - to be productive at home or on the go. Remote access technologies - like VPN (virtual private network) and RDP (remote desktop protocol) - are routinely being stretched for use cases far beyond what is secure.

It is easier than ever for attackers to find these security gaps and deliver malicious payloads, including ransomware.



94% of companies experienced a business-impacting cyber attack or compromise over the last year²



ALMOST 800k A record-breaking number of cybercrime complaints to the FBI in 2020³



69% YoY increase in FBI complaints³

2- The Rise of the Business Aligned Security Executive.
Forrester Consulting (commissioned by Tenable), August 2020

3- 2020 Internet Crime Report (ICR), FBI, March 2021.



A Multicloud World, with Multicloud Challenges

The cloud risk surface vastly expanded during the recent accelerated period of digital transformation. Today, most organizations are not merely in 'a' cloud—they are in many clouds (PaaS, IaaS), and their end users consume ever more SaaS applications, much of it occurring as shadow IT.

IT teams are struggling to control security across the complex environment of managing across multiple clouds, each with their own shared responsibility models and native toolsets.

Additionally, most companies are not 100% cloud – they operate with a hybrid model that includes an on-premises infrastructure, often based on legacy technology.

Attackers can leverage powerful, free tools, such as Shodan, to zero in on unprotected cloud assets and accounts. Control planes, which govern the entire cloud infrastructure, are often inadequately locked down or exposed to the Internet, leaving them vulnerable to brute forcing attacks and other exploits.

Lack of proper controls also result in misconfigurations that can cause outages or expose buckets of data.





in threat activities
waged on cloud
services by external
actors in early 2020⁴



Growth of Unsecure Remote Access


Over the past decade, most IT security breaches have been remotely perpetrated. While remote access provides a necessary convenience for employees, contractors, vendors, and auditors, it also enables threat actors to bypass all the physical controls and to potentially obtain direct access to resources and data. Thus, remote access has been the path of least resistance to the identities, access, and data that threat actors seek.

Unprepared for a remote worker surge, IT teams hastily stood up new remote access pathways to maintain productivity, while accommodating social distancing directives.



Today, organizations are routinely stretching tools like VPN and RDP far beyond their safe and proper use cases.

For instance, VPNs should never be used on employee or vendor personal devices because they cannot provide the granular access controls necessary for privileged sessions. This haphazard remote access infrastructure, initially expected to be a short-term solution, persists for many organizations and creates a tantalizingly simple attack vector for cybercriminals to exploit and land an initial foothold.





[Internet-facing RDP ports increased by 50%](#) in the early months of the pandemic to hastily support work-from-home (WFH) initiatives. RDP exposed to the public internet is a well-known security taboo, but it routinely happens, and often with the most sensitive of resources. Improperly used and inadequately secured RDP played a huge part in throwing open a wide door for ransomware, malware, phishing, and other attack vectors over the past year.

Organizations have leaned heavily on VPN over the last couple years to quickly expand remote access, yet it is a dangerous mismatch for many use cases, such as for vendors, privileged users/sessions, and users operating on BYOD.

VPN technology was built to provide access and to protect data that is in transit to outside the traditional company network, and it should be treated as more of a business enablement tool than a cybersecurity tool.

Because VPNs typically grant open network access, they dangerously assume the trustworthiness and uncompromised nature of anything in the VPN. That itself is a serious security oversight that violates zero trust principles.

Your security may ultimately only be as good as that of the external endpoint or user you are allowing to tunnel into your environment.

RDP was implicated as one of the most common methods of breaching a network in cases we were called in to investigate, which is why shutting off the outside world's access to RDP is one of the most effective defenses an IT admin can take.

Andrew Brandt, SophosLabs
Principal Researcher

[[Sophos News, June 2021](#)]





Lack of granular controls and visibility into VPN tunneling sessions is only part of the problem. Dozens of VPN vulnerabilities are being exploited, resulting in major business and government breaches.

Compounding this issue is the reality that VPN device and software patching is often forgotten or ignored. Those companies that require VPN access for employees to do their jobs often meet opposition to VPN patching maintenance windows, or even to replacing older VPN technology.

Hackers know that, if they can breach a VPN, in many cases, they no longer have to worry about traditional security controls, such as firewalls—they have complete access to a company's network.

Firewalls can't do much to help block unwanted traffic when you openly grant network access through a VPN. Additionally, VPNs are complex to get right, and they are often misconfigured, creating exploitable gaps for attackers to gain access through—especially when trying to provide granular access to large quantities of users.

Remote workers also pose many compounding risks related to remote access itself, including:

- ▶ Using insecure home and public Wifi networks
- ▶ Utilizing personal devices (BYOD) that lack adequate hardening and other basic security protections
- ▶ Sharing devices with others in the household for work, school, and leisure
- ▶ Moving back and forth between multiple locations, whether it be home, office, or another space





Increase of Vulnerabilities Everywhere

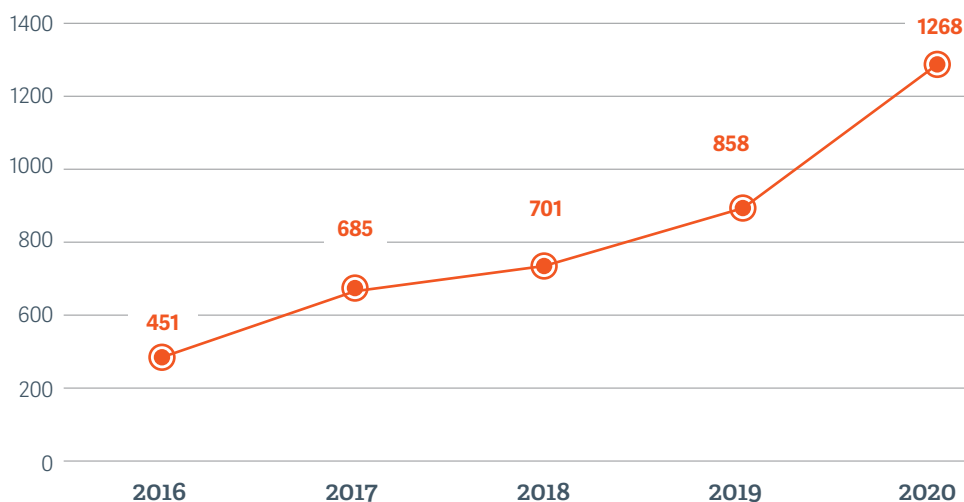
That attackers are leveraging known vulnerabilities is not new—it's one of the oldest IT security truisms. However, this practice continues to give attackers a high rate of success and is a common component of attack chains.


In late 2020, the [FBI and CISA warned](#) that advanced persistent threat (APT) actors are targeting government networks, critical infrastructure, and election organizations with chained vulnerability cyberattacks. These attacks were stringing together legacy vulnerabilities to achieve a foothold and continue to progress an attack.

Such attacks could easily be thwarted at multiple stages by patching alone. However, zero day vulnerabilities can only (potentially) be mitigated by other tactics (such as privileged access management, hardening, etc.) until a patch is available.

The latest edition of BeyondTrust's [annual Microsoft Vulnerabilities Report](#) found that total published Microsoft vulnerabilities reached an all-time high in 2020, leaping 48% YoY. This finding further validates the notion that vulnerabilities and the attack surface are undergoing rapid expansion, partly due to the “quantum leap” in digital transformation.


Published Microsoft Vulnerabilities in 2020





The Explosion of Unmanaged Privileged Identities, Access, and Sessions

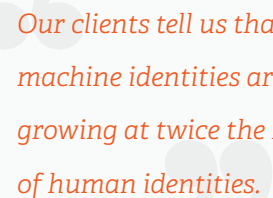
Another noteworthy finding from the 2021 Microsoft Vulnerabilities Report was that, in 2020, “Elevation of Privilege” was the most common Microsoft vulnerability, comprising 44% of all vulnerabilities.



Elevation of privilege vulnerabilities tripled from 2019 to 2020.

The more privileges a piece of software or application, user, account, or process has, the greater the potential for abuse, exploit, or error. Today, many planes of privileges are being created at tremendous scale due to digital transformation, cloud expansion, virtualized environments, IoT, edge computing, shadow IT, etc.

Human and machine privileges—long a security weak spot—are only getting more challenging to discover and control across this vast, decentralized IT landscape because they can truly reside anywhere.



Our clients tell us that machine identities are growing at twice the rate of human identities.

***The Forrester Wave™:
Privileged Identity
Management, Q4 2020.
Forrester Research***

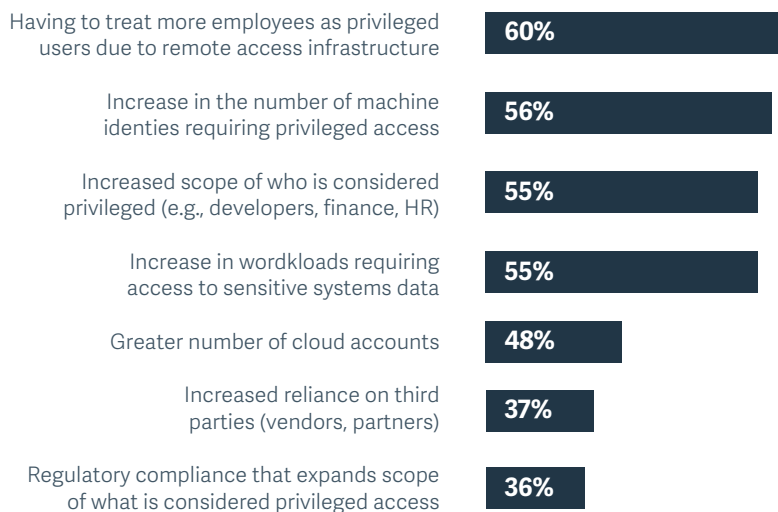


In the event of a cyberattack, the difference between an attack being contained and an attack succeeding and spreading often comes down to whether the attacker is able to achieve lateral movement.

This typically requires a privileged account or the exploitation of a critical vulnerability. Access to a privileged account can also make it easier for an attacker to perform port scanning and leverage native system tools to perform reconnaissance, clean up their tracks, and achieve further privilege escalation.

In a study [BeyondTrust commissioned from Forrester Consulting](#), the majority of organizations surveyed predicted an increase in privileged identities and privileged sessions over the next two years. This increase is largely being driven by aspects of digital transformation.

Why do you expect the number of privileged sessions (human or machine) within your organization to increase in the next two years?



Base: 241 IT security and operations professionals in NA, EU, or APAC

Source: A [commissioned study](#) conducted by Forrester Consulting on behalf of BeyondTrust, June 2020





Supply Chain Fragility, Critical Infrastructure at Risk, and the Interconnectedness of Everything

Over the past five years, supply chain attacks, which compromise trusted software or hardware to infiltrate many more victims, have been on the rise, hitting a spectacular crescendo in 2021.

Yet [Gartner expects 45% of organizations worldwide](#) will incur attacks on their software supply chains by 2025, a three-fold increase from 2021.

By compromising the weakest link – a remote worker, contractor, inadequately hardened system, overprivileged user, unmonitored machine identity, unsecured ports, or VPN vulnerability—an attacker can infiltrate an organization and compromise software being used by thousands of customers, as happened with the SolarWinds and Kaseya breaches, and so many others.

Much of what is being called the “new normal,” is not completely new – it’s just more pronounced.

Highly disruptive and widely reverberating supply chain and critical infrastructure breaches have underscored the interconnectedness and, consequently, the fragility of everything.



Another challenge with broad implications is that parts of OT and ICS (industrial control systems) are increasingly connected to the Internet and easily discoverable, potentially jeopardizing security for the entire critical infrastructure, much of it legacy IT.

[The Claroty Biannual ICS Risk & Vulnerability Report: 2H 2020](#) found that 70% of identified flaws in ICS can be exploited remotely, which demonstrates that these systems are typically no longer fully air-gapped and isolated from external cyberattackers.

In 2021, the world has been shaken by attacks like the water poisoning attempt at a Florida water treatment plant (Oldsmar) and the Colonial Pipeline breach, which took 45% of the fuel supplied to the U.S East Coast region completely offline for months, inflicting widespread disruption and fuel price hikes.

OT systems can be particularly difficult to patch due to the legacy nature of the technology, the environmental complexity, and the pain and costs of a potential disruption. So, it's particularly important for these systems to diligently apply proper segmentation, privileged access management, password management, and other hardening and security best practices.

Also, OT doesn't just pertain to things like utilities and factories anymore. IoT and the proliferation of "smart" things mean industries and businesses, including real estate management companies that may be required to manage smart buildings, need to consider security vulnerabilities and exposures in a way they haven't before.

In 2020, 54% of all Dragos service engagements included a finding about shared credentials in OT systems, and 100% of Dragos incident response (IR) engagements involved shared credentials that were exploited for lateral movement. Further, 88% of service engagements also included a finding about inadequate network segmentation.⁵



Shifting Physical Security Threat

Finally, organizations are facing a heightened physical security threat, not to corporate office environments and server rooms, but rather to remote and mobile endpoints, many of which access and store sensitive data and routinely perform privileged activities.

These devices—laptops, smartphones, tablets, and more—may be:

- ▶ In households shared with roommates or families
- ▶ In high-theft public spaces targeting mobile phones, tablets, and laptops
- ▶ Compromised electronically, such as by SIM jacking, creating a physical electronic clone

While the theft and BYOD risk of mobile (smartphone, laptop, etc.) has existed and been rising for more than a decade, today the scale is many multiples higher. An attacker can now assume that an employee's corporate device is likely at their home.

If a malicious insider has access to a laptop, or the device has been stolen from someone's residence, there is nothing stopping the threat actor from disassembling it and removing critical components, such as a hard drive, or perhaps even adding malicious hardware for surveillance. When the employee is at home or in a public space, there are typically no advanced physical protections to prevent this type of device theft or manipulation.



The Attack Surface is Vastly Increasing

More Vulnerabilities

More Remote Access

More Privileges

More Shadow IT

More BYOD / BYOT

More Cloud

More Digital Transformation

More Identities (human, machine, etc.)

More Connectedness of Everything

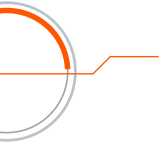


Threat Vectors Heating Up

The vastly increasing attack surface creates a fertile environment for a diverse array of threat actors and attack activities.

In this section, we will highlight three of the most prominently increasing threat trends—phishing, fileless attacks, and ransomware.

Phishing Attacks Are Surging



➤ “As a result of a greatly expanded digital attack surface, phishing attacks are up 600%, including Covid-19-themed phishing attacks aimed at workers mixing personal and work devices over non-secure Wi-Fi networks. A majority of those remote work-related breaches emanated from a lack of visibility by administrators over employee access policies and vulnerable endpoints.”

Chuck Brooks,
Cybersecurity Expert, Georgetown Faculty Member.
BeyondTrust Microsoft Vulnerabilities Report 2021

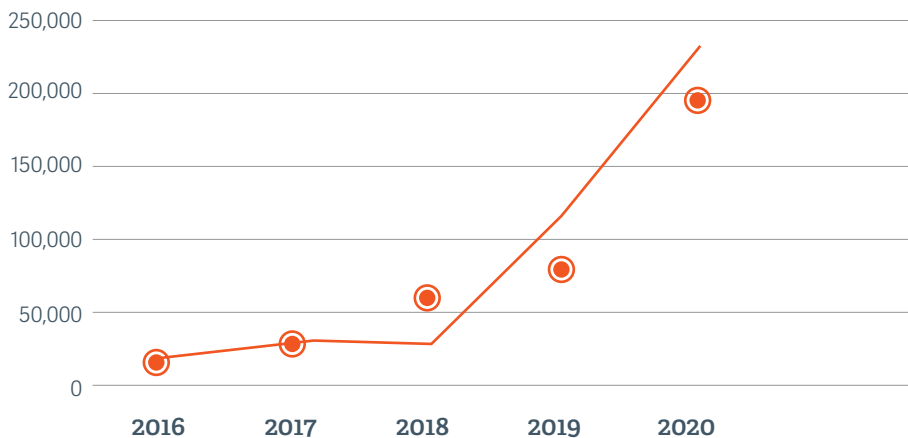




Phishing attacks are on a precipitous upward trajectory, with threat actors going “all in” on these social engineering exploits against the many vulnerabilities and security gaps that have been created by a massive remote workforce.

Phishing, social engineering, and drive-by compromise were the most common initial access techniques observed by [BeyondTrust Labs](#) from May 2020 – May 2021. Phishing has persisted for years as a leading vector to initially compromise an environment, such as with a malicious link or attachment, as well as for information gathering that can later be used to exploit a weakness that presents itself.

Number of phishing crime complaints to the FBI Internet Crime Complaint Center



Includes complaints for Vishing, SMishing, and Pharming

Source: Internet Crime Complaint Center

The expectation of receiving legitimate communications via email—often from unknown or unanticipated sources—makes it easy for an attacker to achieve a high success rate, especially if they can tailor an attack based on available research or leaked data on their target.





Fileless Attacks are Soaring

Fileless attacks, often called living off the land (LotL) or zero footprint attacks, experienced a meteoric 888% rise in 2020. These tricky threats often use a victim organization's own legitimate tools (PowerShell, Wscript, etc.) against them.

Fileless malware are key to the success of advanced persistent threats (APTs), and were a notable part of major breaches, such as SolarWinds, in recent years. Living off the land threats excel at staying under the radar and avoiding detection, while advancing the motives of an attack.

“The general trend we are observing has been toward using native tools to perform fileless attacks in the initial stages until a strong foothold and persistence mechanism is established and security controls have been disabled.”

James Maude,
Lead Cybersecurity
Researcher,
BeyondTrust Labs,
Malware Threat Report
2021





Ransomware is Winning

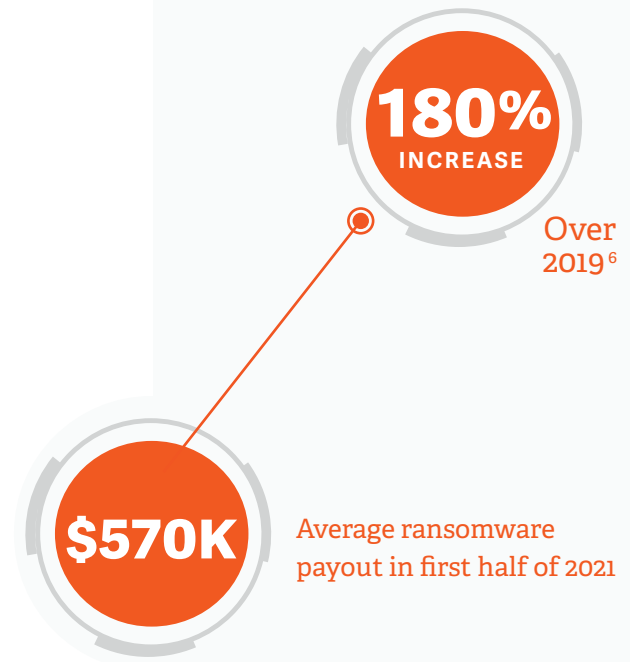
Ransomware attacks [surged 150% in 2020](#), with a Tenable study reporting that [35% of breaches are now ransomware-related](#).

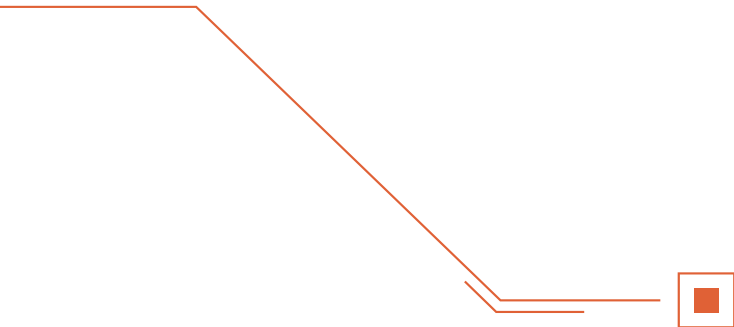
In their [Q4 2020 Internet Security Report](#), WatchGuard Technologies report a 33% year-over-year increase in ransomware families. Why? Because the economics of ransomware continue to reward ransomware operators.

According to [Deloitte](#), some common cybercrime businesses can be operated for as little as \$34 per month and could return \$25,000. Put simply, cybercrime has a low barrier to entry, coupled with a potentially lucrative ROI—and it's generally all tax free!

In 2021, numerous ransomware victims and their insurers made eyepopping 7- and 8-figure payouts, including \$4.4 million (some of which has since been recovered thanks to the government) by Colonial Pipeline and \$11 million by meat supplier JBS.

Pre-packaged exploits and, increasingly, ransomware-as-a-service (RaaS) make it easy for threat actors. They simply shell out a few bucks (typically in cryptocurrency), point, and fire. With some tools, they don't even have to aim—the malware opportunistically seeks out and crawls through vulnerabilities wherever it may happen to run into them. **It may take just a hit or two to pay off.**






Why Is Ransomware Winning?

- 1 Insecure remote access
- 2 Risky user behavior
- 3 Poorly managed privileged access
- 4 Ineffective (or lack of) application control
- 5 Unpatched vulnerabilities
- 6 Poor credential management





How to Tip the Scales Back on Cyber Attackers



➤ In cyberspace, there exists no safe harbor. Every organization with a digital presence is exposed like an island amidst an angry, implacable ocean that seems to send wave after wave of cyberattack.

The year 2021 arguably stands out as the most brutal and shocking in terms of cyberattacks. However, we're also seeing some promising signs that the tide can be turned.

President Biden's [Executive Order \(EO\) on Improving the Nation's Cybersecurity](#) is one call to action helping marshal resources and collaboration across the U.S., and governments in other regions are reacting similarly.

In October 2021, the U.S. also [convened a multinational summit](#) on the topic of combatting ransomware, involving over 30 nations. An astonishing 96% of public sector IT security leaders say their cybersecurity budget has adequate funding, and 83% indicate confidence that the American Rescue Plan (ARP) stimulus will boost government cybersecurity, according to BeyondTrust's [2021 Cybersecurity Trends in Government Report](#).



Government and regulatory bodies have a huge role to play in helping take down and prosecute cybercriminals and criminal networks, while putting forth standards that improve the cybersecurity of the entire internet-connected ecosystem.

Moreover, government officials have signaled renewed vigor in their approach to dismantling cybercriminal syndicates—whether backed by run-of-the-mill, profit-seeking hackers, or nation-state threat actors.

With that said, organizations with a digital presence need to proactively own their journey in addressing security gaps and managing their threat surface.

An important shift is already underway. Identity-centric security and zero trust are rightly being focused on as critical for protecting against the modern, emerging threatscape.

These controls can deliver substantive benefits in the form of reduced cyber risk, while making IT environments more adaptable and resilient, and better poised to address the demands of the future.



80% of IT security professionals say the shift to remote work is increasing the focus on identity security



90% of IT security pros agreed with the statement, “Identity management used to just be about access, now it’s mostly about security”



93% of IT security professionals say zero trust is strategic for securing my organization⁷



7

Cybersecurity Survival Strategies

Now that we've covered how work paradigms, the threat landscape, and how cybercriminal tactics are shifting, let's review our top IT security strategies and survival tips.

These **7 strategies**, each broken down into survival tips, will help you recalibrate your security and better protect your data and digital assets.



1

SURVIVAL STRATEGY

Protect Privileged Identities

The identity challenge is the most important security problem for organizations to solve across cloud and on-premises environments.

No identities are more critical to protect than privileged identities—whether associated with humans or machines, employees or vendors, and whether they are persistent or ephemeral.

The credentials for these privileged accounts can fast-track access to sensitive data and open up lateral pathways that enable an attacker to broaden the sphere of attack and escalate privileges.

Once inside a victim's environment, attackers can also exploit inadequate credential security controls to hijack additional accounts and move laterally or elevate access. **Forrester Research has estimated at least 80% of data breaches are connected to compromised privileged credentials.**

Credential-based attacks (i.e; credential theft, password reuse, pass-the-hash, etc.) continue to be a key element in most breaches. Prominent examples include the Colonial Pipeline and Verkada attacks. Both multi-step attacks leveraged inadequately managed privileged credentials to gain initial access in the victim's environment.

Confidence in securing employee identities dropped dramatically, falling from 49% in 2020 to only 32% in 2021.⁸



- The Verkada attackers found super admin credentials embedded in a python script on a publicly exposed Veracode Jenkins Plugin on the Verkada server.

These credentials should have been replaced (such as with an API call) and vaulted via a privileged password management solution.

In the case of the Colonial Pipeline breach, the Darkside cybercriminal group found stolen credentials that provided access on a dormant Colonial Pipeline VPN account that was still connected to the network. It's likely the credentials found by Darkside were re-used across multiple systems.

This early attack stage could have easily been prevented by at least 3 different privileged password management controls:

1. Enforcement of unique credentials to prevent compromised credentials from being used across multiple accounts and assets
2. Frequent rotation of credentials to limit the window of time a stolen password remained active and could be used to gain access
3. A review of privileged access; the findings could have prompted security teams to either disable the dormant VPN account, put additional workflows around using it, or implement alerts around its use to ensure close monitoring

In a [report](#) from the Identity-Defined Security Alliance (IDSA), timely reviews of privileged access was actually the most-cited (50% of respondents) security control that could have prevented or mitigated a breach experienced by the respondents.

Often, too much access is provisioned by default, or the access is open-ended (standing privileges), when it should only be provisioned just-in-time when certain contextual parameters are met, and then revoked when the task is completed, the context has changed, or a certain amount of time has elapsed.





Privilege creep is another risk that is easy to overlook. Roles change, people accumulate privileges, or people leave the company, yet access and accounts remain active. By routinely re-examining access usage and roles, you can fine-tune provisioning to ensure the organization adheres to the principle of least privilege (PoLP).

For instance, if an account with privileged access has been unused for a month, it's possible it is no longer needed and can be removed, eliminating risk. Or, if the account is rarely used, and only for very highly privileged activities, it may make sense to incorporate additional workflows to grant usage for the account and to send alerts to others when the account is being used. This will allow it to receive closer surveillance.

Even absent the three controls cited above, the Colonial Pipeline attack could still have been thwarted at many stages, particularly by endpoint privilege management controls, which include least privilege enforcement and application control. Yes, breaches can happen, and often threat actors do need just one way in, but many privileged access and other controls typically need to be absent or mis-applied for an attack to reach the devastating level of the Colonial Pipeline breach.

Some non-human (also called machine) accounts, such as service accounts, play a critical role in running programs, applications, and automation workflows. Machine accounts used for automation can be particularly tricky, or impossible, to manage manually due to the potential impact on uptime if password change propagation is not rapidly synchronized across all the places where the account is referenced. Thus, many organizations neglect managing these accounts altogether, hoping other layers will impede an attacker from reaching the account.





Non-human accounts are often over-provisioned with excessive privileges. DevOps tools and CI/CD workflows present similar challenges and risks.

To prevent account hijacking, organizations must automate and centralize the lifecycles for privileged credentials, keys, and secrets.

SURVIVAL TIPS

- **Automate discovery and onboarding of all privileged identities** (human/application/machine) and assets to eliminate privilege blind spots and bring shadow IT under control.

- **Vault and manage all privileged credentials** (passwords, keys, and secrets) according to password security best practices. These practices should include enforcing password complexity and uniqueness, rotating credentials, and injecting them directly into sessions—never revealing them to the end user—whether employee, vendor, or machine. Enforcing capabilities, such as unique passwords and [password rotation](#), help prevent against password guessing attacks as well as re-use attacks. By rotating (changing) a credential, such as after each use in the case of one-time passwords (OTPs) and dynamic secrets, even if a password has been compromised, it has expired by the time a threat attacker tries to use it.

- **Enforce adaptive access controls**, approving or disallowing access requests just-in-time based on context, and revoking access once an activity has been completed, context has changed, or a certain amount of time has passed. A JIT access model eliminates open-ended privileged access, vastly condensing the time during which an account is privileged and, thus, poses a privileged attack vector risk. However, service accounts should not be delegated to any form of JIT access model.





- **Continuously monitor privileged identities and any session involving privileged activity**, whether by human, application, or machine. Monitoring should include performing screen recording, command logging, scripts executed, and screen outputs. Anomalous activity should be flagged, with the ability to pinpoint, pause, and terminate suspicious sessions in real-time. Privileged access should also be periodically reviewed so adjustments to access, as well as its monitoring, can be made as necessary.
- **Enforce multi-factor authentication (MFA)** during login, upon password checkout, and at privilege elevation — anytime there is a new request. This provides added confidence that an identity engaged in a privileged session is who they say they are, and who you expect them to be.
- **Eliminate shared accounts** to ensure clear oversight and auditability into user activities performed by each identity and their associated accounts. When shared accounts are present, it muddles the audit trail and can make it impossible to know which identity did what with an account. Shared accounts also can complicate your ability to achieve various compliance initiatives.
- **Eradicate embedded passwords** in IoT and other devices, applications, scripts, and DevOps tools, and replace them with secure API calls or dynamic secrets. This practice would have eliminated the embedded python script threat vector that allowed the Verkada attackers to gain their foothold.

Key Takeaway

Many of the above protections, such as MFA, just-in-time access, adaptive access, and continuous monitoring, will also help enable zero trust.

86% of IT and security decision-makers say they are investing more in PIM (privileged identity management) over the next two years to address the risks related to remote working. ⁹



2

SURVIVAL STRATEGY

Secure Remote Access

Access to sensitive resources, control planes (cloud, virtualization, DevOps), or to perform privileged activities should be locked down and tightly monitored so it is not exposed to brute-forcing and other attacks.

Another concern is that, when credentials are being entered remotely, they are exposed to the local computer—and to any malware or attack (like man in the middle) that can sniff them out.

Ultimately, the path forward to addressing these challenges involves extending privileged access management best practices (least privilege, privileged password management, session monitoring/management, etc.) beyond the perimeter.

Traditional remote access technologies (VPN, RDP, VNC, etc.) lack granular access controls and session visibility, creating dangerous security holes when extended for many of today's remote working use cases.

➤ In February 2021, a Florida water plant (Oldsmar) was compromised remotely, and the attacker attempted to modify the water's chemical makeup. Researchers at [CyberNews found 11 breached credentials](#) linked to the water plant from 2017, as well as 13 sets of credentials right before the attack.

Apparently, all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed. The attacker also leveraged one of the plant's consumer-grade remote access tools to gain access to the plant's SCADA controls, then subsequently changed the level of sodium hydroxide in the water (commonly known as lye), from 100 parts per million to 11,100 parts per million.

The plant had actually stopped using the TeamViewer remote access tool six months prior, but still left it installed. Luckily, a plant operator noticed the modification in time to revert the change before this breach jeopardized the health of the community.



SURVIVAL TIPS

- **Broker all connections through a single access pathway**, encrypt all traffic, and make every remote connection outbound. These controls help minimize who can attempt to login, while putting distance between remote access and internet-based threats.
- **Proxy access to control planes and other critical software** to segment and isolate remote access traffic. In addition, admin access should be discoverable only to authorized admins.
- **Enforce network zoning and segmentation** to isolate and protect the new attack surfaces created by digital transformation and cloud deployments. This also helps ensure sensitive software, applications, and environments do not encroach on each other.
- **Enforce least privilege access controls**, with just-in-time provisioning, to all remote access. This is a powerful, and necessary, ability to stop attackers and malware from gaining a foothold, as well as from performing lateral movement. Restricting privilege to the minimum necessary also helps keep vendors and other remote workers honest, as they can only access what they need to accomplish their work.
- **Automatically inject managed credentials** into remote sessions to prevent end users from ever knowing or touching the login credentials. This helps ensure strong password security practices are used for all sensitive remote sessions—even for vendors/third-parties.





- **Implement BYOD management** to keep devices secure by isolating and protecting apps and content accessed in the workspace. This necessitates a shift from mobile device management (MDM) to enterprise mobility management (EMM) that can not only protect the device, but also the individual applications and the data contained within.
- **Provide application-level micro segmentation** that prevents remote workers and vendors from discovering or executing applications and other resources they are not authorized to access.
- **Monitor, manage, and audit every remotely initiated privileged session** via screen recording, keystroke logging, and other technologies. This delivers a strong level of oversight and protection that is sorely lacking with VPN and other remote access technologies, ensuring that you always know what identity is logging in remotely and what they are doing with that access.

Key Takeaway

Applying many of these practices will not only greatly reduce your organization's risk of giving attackers an easy foothold in your environment, but they also provide potent defense against lateral movement. In addition, each one of these tips is an essential component of enabling a zero trust architecture for remote access.





3

SURVIVAL STRATEGY

Apply Endpoint Privilege Management (Least Privilege & Application Control)

A least privilege security posture can not only outright eliminate many types of malware and other attacks from executing and gaining a foothold, but it can also maroon attackers who do gain a foothold by sharply reducing the potential for privilege escalation and lateral movement, key phases of the cyberattack chain.

70% of attacks today are reported to involve some form of lateral movement.¹⁰

Restricting software and system privileges to the minimal range of processes required to perform an authorized activity also reduces the chance of incompatibility issues; protects organizations from rogue, compromised, or misused applications; and reduces the risk of downtime, improving overall operational performance.

Applying the principle of least privilege (PoLP) is one of the most powerful and well-recognized ways to prevent malware infection, protect against internal and external threat actors, and mitigate damage potential from a security incident.



10- EGlobal Incident Response Threat Report, Carbon Black.



- In 2020, [Verkada exposed](#) the live feeds of 150,000 security cameras used by their customers, including jails, hospitals, women's health clinics, psychiatric facilities, police departments, and even companies like Tesla. As detailed earlier, the Verkada breach originated via compromised super admin credentials that were found embedded in a python script that was remotely accessible. The threat actors obtained "root" access to the Verkada cameras using built-in functionality that escalated their privileges to "Super Admin." This superuser/root account permitted access to all of Verkada customers' camera feeds, potentially jeopardizing security and privacy at every customer environment.

Many least-privilege controls (removing admin rights, etc.) would have helped prevent or mitigate this breach, as would enforcing separation of privilege and separation of duties. No one account should wield control over so many different customer accounts and have such high-level privileges across so many systems. Rather than having one superuser account perform all of an IT admin's duties, implement separation of privileges and duties across different accounts, with each account requiring unique login credentials and being used only for a specific set of functions/tasks.

SURVIVAL TIPS

- **Enforce least privilege across your environment.** Eliminate local admin rights, server admin privileges, system, and application privileges to the least amount necessary. Access should be granularly controlled and only elevated just-in-time for the moments needed. Least privilege should be enforced across all endpoints (Windows, Mac, Unix, Linux, network devices, etc.), as well as on-premises, cloud, and hybrid environments. Eliminating admin rights alone translates into a significant risk reduction across many platforms, even absent an appropriate patching process. In 2020, 56% of all Critical Microsoft vulnerabilities, and 87% of Critical vulnerabilities in Internet Explorer and Edge, would have been mitigated by removing admin rights, as we published in our 2021 Microsoft Vulnerabilities Report.
- **Assign specific Unix and Linux commands** that IT administrators can execute and run elevated without needing sudo or root. Also provide command line filtering and a policy language that can elevate commands via least privilege and inspect all the options and switches. This allows the identification of malformed or inappropriate commands, which could cause downtime of critical software and expose attack vectors that can be exploited.





- **Enforce separation of duties and privilege separation** to limit the privileges associated with any account or process. When applied to users, this involves segmenting privileges across separate users and accounts, and ensuring certain duties can only be performed with specific accounts and identities. Thus, if one account is compromised, the range of privileges it affords the attacker is restricted in scope. Separation of privileges helps contain intruders close to the point of compromise and restricts lateral movement.

- **Apply advanced application control and least privilege application management** to ensure only approved applications, and the allowed subfunctions within those applications, can run within the proper context. By layering application control on top of privilege management, critical functionality in the operating system is trusted by default (users without privilege cannot introduce new code to directories like Program Files, Windows, System32, or Drivers). This makes it a pragmatic approach because it only needs to be applied to specific directories and files, where threat actors typically 'drop' and execute their payloads. This type of control would also prevent unsigned binaries from executing on the system, as used in Darkside malware attacks.

- **Protect against misuse of trusted applications** by applying context-rich privileged access security controls, such as content and application control rules, and control over launch of child processes. This helps protect against tricky fileless attacks, often part of advanced persistent threats and sophisticated attacks (SolarWinds, Darkside, etc.) that leverage Powershell, Wscript, Cscript, Word, and other legitimate tools.





Key Takeaway

Most of these least privilege controls are pivotal to enabling a zero trust environment. In the past year, many of the above controls would have helped dismantle large-scale attacks at multiple stages—including Colonial Pipeline and the Verkada attacks, as well as countless smaller breaches and security incidents.

- The SolarWinds Orion supply chain attack was particularly devastating because the Orion application needed unrestricted access to work. Since the Orion application itself was compromised, threat actors leveraged this unrestricted privileged access throughout victims' environments using the application. This attack demonstrates why it's essential for organizations to identify and address over-privileged applications, and wherever possible, to implement least privilege application management. However, since many legacy applications (i.e., SolarWinds Orion) may not work without these high levels of privilege, enterprises and agencies should either implement more layers of mitigation, or discontinue use of the software.





4

SURVIVAL STRATEGY

Apply Hardening and Vulnerability Management

Remote and BYOD endpoints pose a significant security challenge with regards to how configurations, controls, and patches are implemented.

However, enforcing least privilege and removing admin rights, as covered earlier, is an essential control that can help mitigate these risks.

In rushing to support a large remote workforce during the early days of the COVID-19 pandemic, agencies and enterprises relaxed their hardening policies.

SURVIVAL TIPS

- > **Harden your IT environment.** Remove unnecessary software, applications, and privileges, close unneeded ports, and ensure endpoints have the latest firmware and patches. Ideally, this is done before an endpoint is ever allowed access to your network. Hardening activities should continue to be performed as needed throughout the device lifecycle and should ensure strong, base configurations. This is especially important because devices may be returning to the office after being at home during coronavirus quarantine.





- **Harden and protect the BIOS.** This should entail enabling password protection for the BIOS and ensuring the password is strong, complex, and most importantly, unique. Moreover, the Boot Device should be configured to only boot from the internal hard disk using UEFI and secure boot—not from external media like a USB device. An external bootable device can circumvent other security controls and even overwrite the operating system. Therefore, it will control how the device can boot up and will remember to use a BIOS password to secure this setting. The BIOS password can be managed by a privileged password management solution.
- **Implement continuous vulnerability management.** Scan, assess, prioritize, and address software, application, and other system vulnerabilities in an ongoing manner. Addressing vulnerabilities can entail patching and/or another mitigation (i.e. a configuration change or use of cybersecurity tools), while accepting a vulnerability could include actions that range from doing nothing to purchasing cyber insurance. Prioritization is a key component of vulnerability management and is essential to effectively addressing the sheer multitude of vulnerabilities that will exist across any moderately complex IT environment. While patching is guaranteed to remediate or “fix” a vulnerability, patching itself is not always a riskless activity—it could cause incompatibilities, software disruption, or could even bring an application or tool out of compliance. That’s why IT teams should seek automated tools that can help them quickly make smart vulnerability management decisions that minimize the attack surface, while preserving uptime.

Key Takeaway



Together, systems hardening, configuration management, and vulnerability management can provide a robust baseline to secure software and protect endpoints.



5

SURVIVAL STRATEGY

Prevent Tampering of Mobile and Remote Endpoints

While some devices could be stolen simply as part of a run-of-the-mill burglary that seeks any valuable items, nation-states and other organized threat actors may target the homes of privileged users as part of cyberespionage. Ensuring the integrity of remote and mobile endpoints, and the data that resides on them, is critical.

Outside of corporate environments, mobile and remote endpoints are more exposed to on-device attacks.

SURVIVAL TIPS

- **Implement disk encryption.** This is the best method for ensuring a threat actor cannot access sensitive data if the hard disk is removed. Even if the device is removed and mounted on an external rig, it cannot be easily accessed since the encryption is typically paired with the original hardware. And if the device is physically stolen, without a password, access is still denied. However, please take note that, for some devices, an administrator password or key is all that is needed to decrypt the disk and provide access.





- **Use embedded hard disks.** These are becoming more common to trim device costs and enable the use of lightweight laptops. This storage medium is not removable like a PCIe or SATA hard disk, but rather the microchips for SSD storage are physically soldered to the motherboard. The downside is that this practice can make it more difficult to legitimately service a device or perform storage upgrades.
- **Seal the device.** The screws that hold a device together can range from Phillips to Torx. Some sizes are standard while others are proprietary. As trivial as this sounds, if the threat actor does not have the tools to open a device, they are less likely to gain access. This is especially true if their access to the device occurs during a short window of time. And, if the screws are sealed with glue or a bonding agent, they cannot be easily removed, making the device nearly disposable, in case of a fault. This is true for any device that the user may need to use while working remotely—from a laptop to hardware-based VPN. If the internals of a device represent a risk, and the risk, fault, and cost model warrants, consider permanently sealing the device from any access.
- **Distribute and require use of computer security cables** to secure a device to a desk or table to prevent theft. Computer security cables consist of a cable, lock (combination or key), and a mounting clip that attaches to the asset to be protected using a standard-size oval connector. Security cables are typically used in areas of high foot traffic or in public locations, but they also provide an effective layer of physical protection for home/remote offices. If the endpoint being used at an employee's home has sensitive information, consider issuing security cables to the user to help prevent theft.





- **Apply BIOS tamper protection.** *Note: this feature is only available from certain vendors.* Tamper protection is typically enabled in the BIOS and has a software component that is loaded onto the operating system. Tamper protection monitors the device for evidence that the device case has been opened or physical components have been removed or changed. If tampering is detected, the software alerts a management platform. BIOS tamper protection should be considered an essential technology for mobile devices used by remote workers. In the absence of tamper protection, consider running delta reports against hardware using your asset management systems to determine if any components have been changed, removed, or added. While this won't tell you if the case has been inappropriately opened, it will help determine if key components have been altered.

Key Takeaway

With thousands to millions of remote and mobile endpoints (whether corporate or employee-owned) used for work, the likelihood of experiencing a stolen or lost device is high. A mix of these anti-tampering controls, combined with a clear and strong device policy on which users are well-educated, is pivotal to preventing and mitigating the impact of device theft and/or tampering.





6

SURVIVAL STRATEGY

Secure and Empower the Service Desk

During the initial phases of the pandemic and social distancing, service desks did what they could, with the tool(s) they had, to help their organizations go remote, but it often wasn't pretty.

And with all the users newly working from home and often using new tools, help desk tickets spiked.

While many of the tools service desks leveraged for the new use cases created scalability headaches, their security risks pose a much bigger concern.

Many organizations have not caught up to the reality that remote support represents a type of privileged access and needs to be treated as such. For instance, service desk technicians are often required to use admin credentials with elevated privileges to resolve support issues.

As remote support and unattended access use cases have exploded, so too has the security risk. The compromise of a consumer-grade remote support/access tool led to the breach resulting in the water poisoning attempt at the Oldsmar Florida water treatment facility.

Service desks require a remote support tool that continuously protects them and the customers (both internal and external) they serve, reduces incident handling time, improves customer satisfaction and first call resolution, streamlines processes, and has synergies with other service desk tools they use.

The pandemic challenged people in all industries, some more than others. In the IT world, arguably no group had more thrust on its plate, nor was more pivotal to a company's ability to adapt, than the service desk.

Going forward, service desks will continue to be leaned heavily on and will play a critical role in keeping organizations secure.





SURVIVAL TIPS

- **Enforce strong privileged access security controls over all remote support sessions.** Sessions should have strong encryption. The remote support tool should be able to work through firewalls—without VPN tunneling—so your perimeter security can remain intact. By using outbound-only session traffic, such as using TCP Port 443, you can also minimize port exposure, vastly condensing the potential exposed attack surface of your support site.
- **Apply client segmentation.** Each remote support customer should be segmented via single-tenant environments, so data is never co-mingled.
- **Implement credential security best practices.** Enable MFA and manage all credentials in a vault. Credentials should be automatically injected into sessions without being revealed to the user or remote support personnel. It's also desirable to enforce different policies for unattended versus attended access.
- **Enable platform-independent support.** Service desk technicians should be able to provide support regardless of either their platform or the end user's platform. The broader the platform support, the better your case for standardizing support by using a single tool to improve incident handling time, technician productivity, and to reap other efficiencies.
- **Streamline workflows and integrate with other service desk tools** to ensure a smooth experience for both the technician and the customer. Your technicians should be able to launch a remote support session directly from the support ticket or change record, automatically update tickets with details from the support session, and include the chat transcript and session recording in the ticket.
- **Finally, by deploying endpoint privilege management in tandem with your remote support tool,** you can sharply reduce IT tickets and unburden the service desk, helping them scale and perform at their best.





7

SURVIVAL STRATEGY

Perform Remote Worker Penetration Testing, Carefully

Problematic, or Non-Permissible, Pen Tests for Your Remote Workforce

First, let's cover the types of assets and scenarios that are typically outside of scope for any corporate remote worker pen testing.

ASSET**Personal, Home-Based Networks****SCENARIO**

Wired and wireless, including network reconnaissance and device inventorying. To pentest these areas, you would need to obtain explicit permission from the end user to inventory, classify, and perform a risk analysis on the networks supporting their home-based environment. Company policy would also have to allow for this testing. Most home users will reject this access request.

Devices Owned By Other Companies

May be using the same network, wired or wireless, due to other family members working from home. This clearly represents a scoping issue and never should be allowed for any pen test.

Remote workers alter the attack surface and create new risks that need to be assessed.

But, what constitutes a valid end-user pen test (penetration test) when the target is not in the physical office?

What exactly are you allowed to test?

Are personal devices off-limits?

You also must consider what permissions you may need to obtain if your penetration test extends beyond the equipment that you've issued, and electronically traverses home networks and consumer internet providers.

**Personal and IoT Devices**

Including personal digital assistants, alarm systems, home automation, etc. Such devices and software represent a potential critical attack vector, such as from vulnerable end-of-life devices. A corporate assessment of these devices is only permissible with the explicit permission of the employee/device owner. Also, keep in mind that the target (device, etc.) may be rendered inoperable from an aggressive pen test.

Personal email addresses that may be on the same BYOD assets

These are off limits, regardless of where the personal device is located. Organizations should enforce use of an MDM or EMM solution to provide email segmentation and data management.

Home Phone Numbers

May also be used by others in the same household as the employee. Will anyone other than the employee potentially answer the phone if it rings? Do not conduct a pen test if you cannot predict the call recipient's identity with high confidence.

Cellular Phone Numbers

When used for answering work calls are a pen testing gray area. If the device owner expenses their cell phone, it is BYOD for business and fair game for a pen test during normal business hours. However, it is still a personal device and the scope needs to be considered—from Vishing to SMishing (voice and SMS phishing)—depending on your business' code of conduct policy and regional laws.

Non-Business Social Media Accounts

This is unchanged with remote workers and should not be considered as a part of any new policies and scope.

While any vector in the above list could be exploited by an attacker, they tend to be off-limits, or at least problematic, for pen testing due to legal ramifications, jurisdiction, property, ownership, and/or local laws. In these instances, organizations can only legitimately perform pen tests if the targeted employee has given explicit consent. It's unlikely that your employee code of conduct and security policies contain provisions allowing pen tests for the above use cases.





The Top, Permissible Pen Tests for Remote Worker Risks

Now that we've covered pen tests that would likely run afoul of company policies, let's explore valid methods for penetration testing remote workers.

ATTACK TYPE VALID TESTING METHOD

Phishing Pen testing using phishing should target all users regardless of role—from executive to receptionist, tenured employees through new hires. Webmail, mobile devices, and mail client installations are all fair game. The scope of phishing pen tests can also encompass specialized attacks, like spear phishing and whaling. Consider not pre-announcing phishing pen tests and potentially leave the scope open to all users, with need-to-know rights only to key staff who might triage an end-user-identified phishing attempt.

Vishing Social engineering that targets users via telephone calls to landlines, cell phones, VoIP, phone systems and applications, and POTS (plain old telephone system) home phones. Depending on how the end user accepts phone calls (and ensuring they are the only one answering the call), vishing provides a risk assessment of how verbal social engineering can be leveraged against the business. Vishing pen testers could pose as clients, vendors, or other employees in distress or in need of information.



**SMishing**

Social engineering using SMS text messages. SMishing is an effective secondary attack vector when disguised as two-factor authentication, or when the CallerID is spoofed to appear like it's coming from a known caller (like an organization's main telephone line) or a local phone number. SMishing realistically only has two attack vectors for a pen tester: replying to a text or clicking on a link. While replies to SMishing attempts may reveal sensitive information, links front-ending fake authentication pages tend to work best when trying to exploit users. These pen tests would be performed on registered mobile devices that are authorized to process work calls and emails. If the device is truly personal and the phone is not registered in the corporate directory, it probably falls outside your scope.

Social Media to Promote Work

Used by employees to promote work events, sales, news, and activity is fair game for a pen test, regardless of whether the targeted employee works from home or not. All pen testers must do is reply to an existing work-related post to begin their attack. In fairness, you will probably find that training end users on this attack method is just as important as with email phishing, particularly if the users are highly active on social media on behalf of the organization.

Remote Access Infrastructure

Encompasses everything from VPN clients to VPN concentrators and dedicated remote access technology used for remote workers to access resources. Do not provide the pen tester with the network topology for remote access. You want the pen tester to attempt to map out the vendors, network, and process for remote access. If the pen tester can accomplish this mapping, then all they need to do is use social engineering or a vulnerability-exploit combination based on vendor or technology to infiltrate the organization. If a threat actor understands how your remote employees gain access at a granular level, it is only a matter of time before they find a weakness and exploit it.



**Remote End Users on Company-Owned Assets**

A valid pen test target, whether they are on-premise or working remotely. You may not be permitted to scan the device via the user's home network, but you can certainly scan the device if a protocol-based network tunneling connection exists. The scanning method is what matters. If you can exploit the end user remotely via VPN, then the pen tester's goal has been achieved. While lateral movement to home devices via pen testing is typically not permissible, lateral movement to other visible devices via VPN is allowed (barring split-tunneling attacks). The pen test must stay within the confines of the corporate network, including VPN tunnels. The pen test must not leverage devices outside of their legal permissions. In addition, if the organization is using remote access technology that doesn't use protocol tunneling, the application itself and supporting infrastructure represent the only valid attack vectors. There is nothing in between to route network traffic—only to render screens and session data.

Businesses need to consider their options and clearly understand what is in scope versus out of scope for a penetration test. While some resources remain off limits for pen testing, you still need to account for that unknown/indeterminate risk in your risk management policy and security operations.

Key Takeaway

Once risks are identified by pentesting, and the nature of them is well understood, your organization can design mitigation plans, such as training, patching, removal of local administrative rights, changing a configuration, bolstering security of remote access pathways, etc.





Recalibrate Your Security with BeyondTrust to Address Today's Threats

BeyondTrust provides a complete **Privileged Access Management platform** that helps implement the secure foundation organizations need to enable remote work and digital transformation, while remaining resilient, adaptive, and protected.

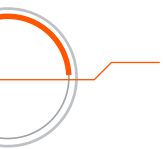
Our PAM solutions provide must-have capabilities, such as **least privilege enforcement, privileged account and credential management, and remote access security**, that are increasingly demanded by cyber insurers and that are integral for reducing cyber risk and cyber liability.

In the appendix to the [2021 Verizon Data Breach Investigations Report \(DBIR\)](#), the U.S. Secret Service commented on how to best protect infrastructure:

"Security postures and principles, such as proper network segmentation, the prevention of lateral movement, least privilege, and 'never trust, always verify' have proven to be strong indicators of an organization's ability to prevent or recover from unauthorized presence in its network environment."

These are all security controls that BeyondTrust excels at helping enforce.



A decorative graphic on the left side of the page, featuring a partial orange circle and a line that extends to the right, ending in a chevron shape.

➤ BeyondTrust solutions support the smart, practical implementation of the NIST (SP 800-207) zero trust principles. Our solutions ensure all access is appropriate, adaptive, granularly controlled and restricted in amount and duration, and documented—regardless of how the perimeter has been redefined.

The BeyondTrust platform is comprised of four solutions:

- ▶ Privileged Password Management
- ▶ Secure Remote Access
- ▶ Endpoint Privilege Management
- ▶ Cloud Privilege Protection

You can deploy these solutions separately, or together as part of our integrated platform, so you can benefit from cybersecurity and workforce productivity synergies.

BeyondTrust solutions can all be delivered on premise, in the cloud, or via a hybrid deployment.





The BeyondTrust PAM Platform



Privileged Password Management

solutions enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities.



Endpoint Privilege Management

solutions combines privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity.



Secure Remote Access

solutions enable organizations to apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.



Cloud Privilege Protection

solutions help organizations pinpoint and mitigate risks associated with cloud access permissions and entitlements across multicloud environments.

ON-PREMISES

CLOUD

HYBRID

Beyondinsight Discovery | Reporting | Threat Analytics | Connectors | Central Policy & Management

If you embrace a proactive cyber risk management approach, you should be continuously asking —

What is the threat actor's path of least resistance, and what can be done to prevent it from becoming an attack vector?

Ultimately, you want a potential threat actor's path of least resistance to be another company or target. However, within your environment, **you must continually reassess where your own paths of least resistance are, and the risk this poses to your organization.**

This assessment will help guide the judicious deployment of technologies or adjustment of settings and infrastructure in alignment with your risk appetite.



> Additional Resources

- WHITEPAPER [The Guide to Multicloud Privilege Management](#)
- WHITEPAPER [A Zero Trust Approach to Secure Access](#)
- BUYER'S GUIDE [Privileged Access Management \(PAM\) Checklist & Buyer's Guide](#)
- BUYER'S GUIDE [Remote Support Checklist and Buyer's Guide](#)



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 solutions 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