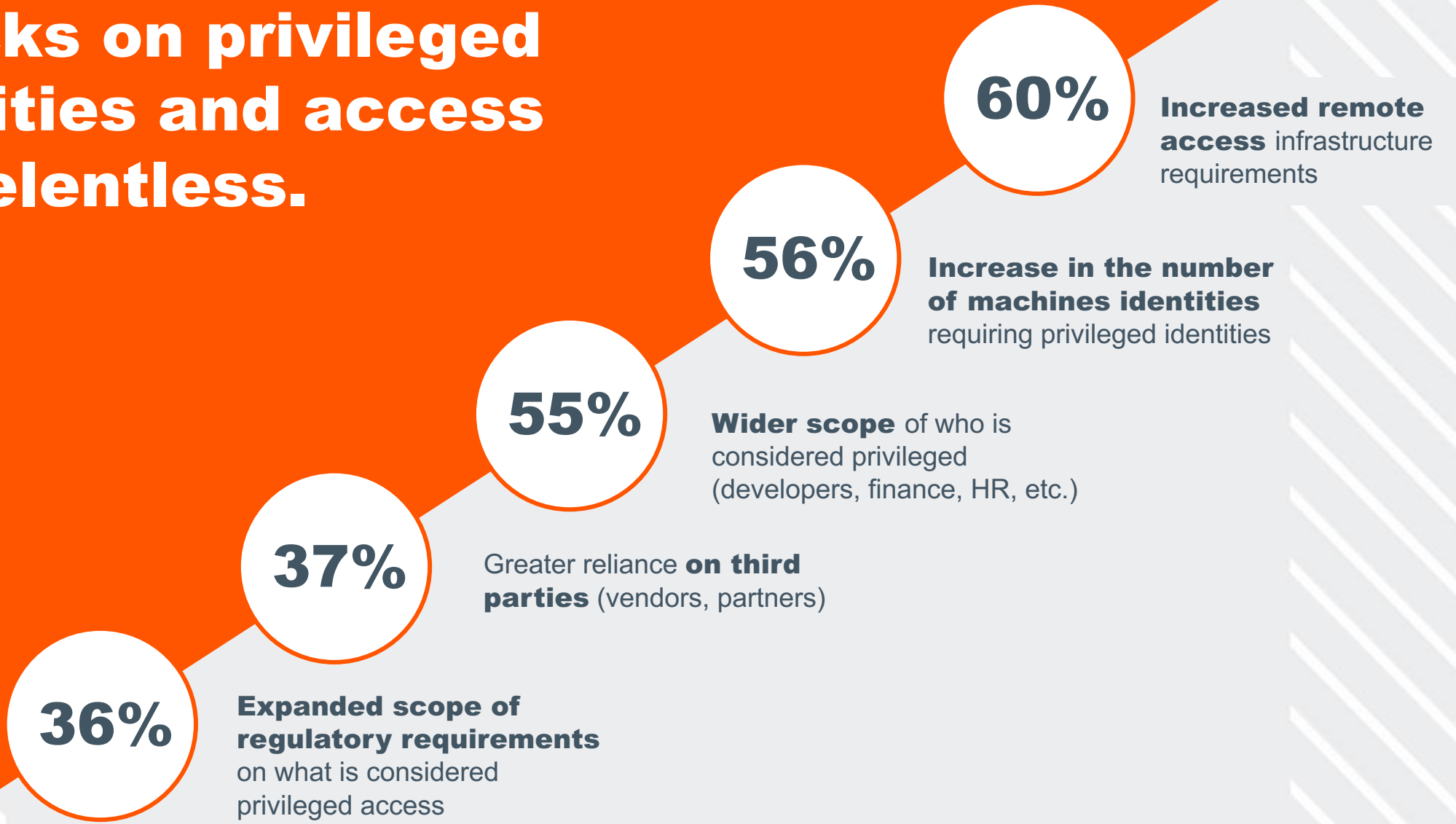
4 CYBERSECURITY SURVIVAL STRATEGIES

RECALIBRATE YOUR SECURITY FOR TODAY'S THREATSCAPE

Attacks on privileged identities and access are relentless.



SOURCE: *A commissioned study conducted by Forrester Consulting on behalf of BeyondTrust, June 2020*

1 Protect Privileged Identities

Privileged identities are the most critical to protect because they fast track access to sensitive data

- ✓ Automate discovery & onboarding of privileged identities
- ✓ Vault and manage all privileged credentials
- ✓ Continuously monitor privileged identities & sessions
- ✓ Enforce multi-factor authentication (MFA)
- ✓ Eradicate embedded passwords

2 Secure Remote Access

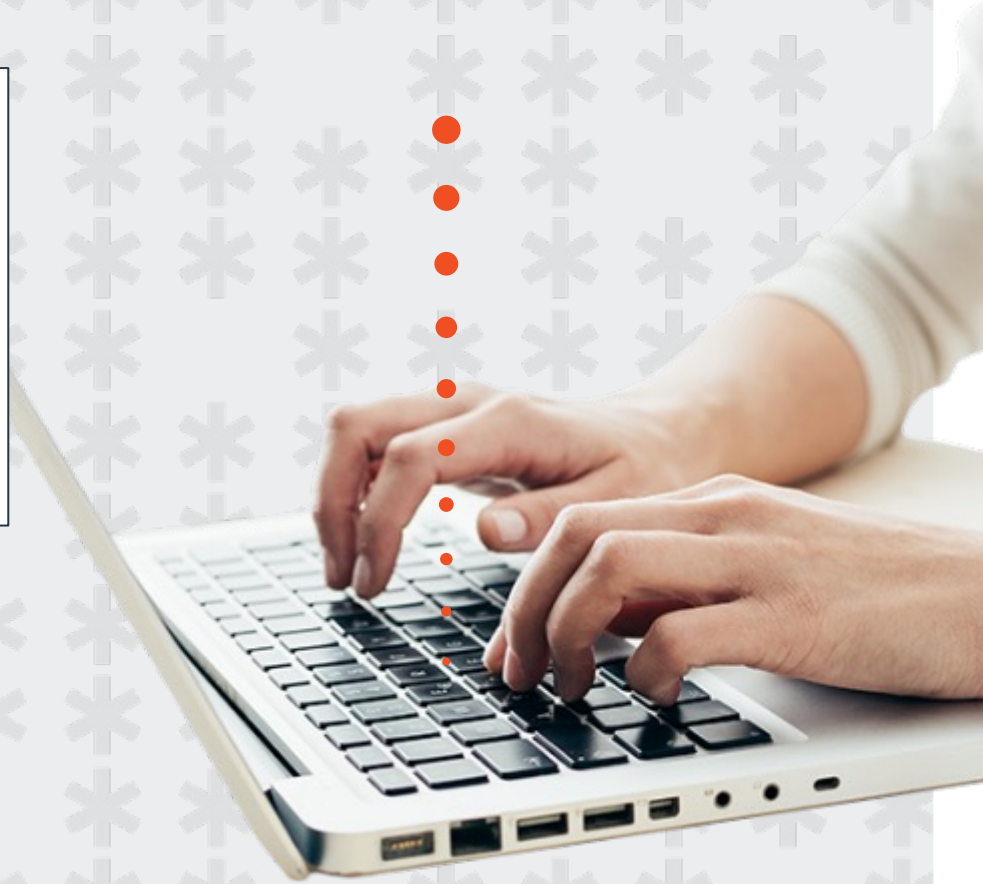
Unsecured remote access is the path of least resistance to sensitive resources and data.

- ✓ Broker all connections through a single access pathway
- ✓ Proxy access to control planes and critical software
- ✓ Enforce least privilege access controls
- ✓ Provide application-level microsegmentation
- ✓ Manage & audit every remotely initiated privileged session

3 Apply Endpoint Privilege Management

Vulnerable endpoints expose organisations to malware, privilege escalation and increased downtime.

- ✓ Enforce least privilege across your environment
- ✓ Enforce separation of duties and privilege separation
- ✓ Apply advanced application control and least privilege application management
- ✓ Protect against misuse of trusted applications



4

Secure & Empower the Service Desk

Without securing and empowering their service desk organisations can face scalability & operational issues.

- ✓ Streamline workflows and integrate with other ITSM tools
- ✓ Enforce strong privileged access security controls over all remote support sessions
- ✓ Implement credential security best practices
- ✓ Enable platform-independent support
- ✓ Deploy endpoint privilege management in tandem with your remote support tool

Candid Security Advice From A Ransomware Operator

YOU CAN'T MAKE THIS UP

An attacker instructing their "customer" on how to prevent a future attack!

"Check the granted privileges for users, to make them maximum reduced privileges and access only to exact applications."

Prepare & Prevent

The attack on critical industry

CASE STUDY: COLONIAL PIPELINE ATTACK

Holding tanks are seen at Colonial Pipeline's Linden Junction Tank Farm in Woodbridge, N.J, in an undated photograph. (Colonial Pipeline/Handout via Reuters)

US NEWS

Cyber-Attack Shuts Down Biggest Gasoline Pipeline in US–Colonial Pipeline

BY REUTERS | May 8, 2021 Updated: May 9, 2021 Print

Disrupted 45% of U.S. East Coast fuel supply for months

Resulted in a $5 million payout by Colonial Pipeline

Colonial Pipeline Breach

Darkside Group

Breaking the Attack Chain

What Happened

Phase 1 – Land	Phase 2 - Expand
• Dormant VPN credentials were stolen • Passwords were reused in multiple accounts • MFA was not in use	• Unsigned binaries execute on the system, security tools disabled, local backups deleted, files encrypted • PowerShell launching with elevated privileges • COM used to perform a UAC bypass

* - assumptions based on typical malware deployed by Darkside

Colonial Pipeline Breach
Darkside Group
Breaking the Attack Chain

Best Practice

- Privileged access reviews and right-sizing
- Credential management and rotation
- MFA enforcement
- Application control can prevent unknown executables from running
- Could have mitigated the UAC bypass attempt by removing the user's admin privileges
- Application control can mitigate this by controlling execution and elevation at a granular level

CASE STUDY: OLDSMAR WATER POISONING ATTEMPT

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town

For years, cybersecurity experts have warned of attacks on small municipal systems. In Oldsmar, Fla., the levels of lye were changed and could have sickened residents.

"This is dangerous stuff," Sheriff Bob Gualtieri of Pinellas County said at a news conference Monday of hackers who remotely accessed the City of Oldsmar's water supply system and changed the levels of lye. Pinellas County Sheriff's Office

Disrupted operations and jeopardized public safety

Oldsmar Attack

Breaking the Attack Chain

What Happened

Phase 1 – Land	Phase 2 - Expand
• Oldsmar credentials were breached (discovered by CyberNews) • Consumer-grade remote support/access tool was compromised. • Oldsmar had stopped using the remote access tool 6 months prior, yet left it installed.	• Unsigned binaries execute on the system, security tools disabled, local backups deleted, files encrypted • PowerShell launching with elevated privileges • COM used to perform a UAC bypass

Oldsmar Attack

Breaking the Attack Chain

Best Practice

- Ensure passwords change routinely.
- Application control can ensure only approved remote access tools that meet security standards can be used.
- Privileged access reviews identify stale passwords, unused/unneeded provisions and addresses.
- Ensure unique passwords for every user/device to prevent lateral movement.
- Identify suspicious actions and pause or terminate in-progress sessions

The evolving threat landscape is creating a new urgency to achieving cybersecurity goals

- Controlling **access** for employees, vendors, remote workers, and machines
- Mitigating **ransomware** attacks
- Supporting **digital transformation** initiatives
- Enabling a **zero trust** posture
- Driving **IT efficiency** and automation
- Maintaining **compliance** and **cyber insurance** policies

Thank You

Scott Hesford
Director of Solutions Engineering, APJ

beyondtrust.com