Today’s news is filled with data breach stories that stem from security gaps introduced by third-party vendors. This isn’t surprising given that the 2013 Trustwave Global Security Report¹ found, “63% of the 450 data breaches studied were linked to a third-party component of IT system administration,” meaning a third party had introduced security deficiencies easily exploited by hackers.

What is surprising is how many enterprises haven’t secured how third parties remotely access their networks.

These third parties—including vendors, service providers, independent consultants, contractors, and partners—need access to conduct essential business and IT operations, but access shouldn’t be as simple as “on” or “off.” In order to conduct business safely, IT organizations must be in control of centralized vendor access pathways that allow them to enforce access control policies and record and monitor all third-party activity.

Here are five actions you can take now that can make a big impact on improving your third-party access security in the future.

1. CONSOLIDATE REMOTE ACCESS TOOLS
How many vendors and service providers have remote access to your systems today? And are they all using the same solution or a bunch of different tools? If you’re honest, it’s likely the latter. If you’re really honest, you may not even know what remote access tools your vendors use or which systems they’re accessing.

By forcing every vendor (and internal employees) to use one, consolidated, company-owned solution to remotely access your network, you will greatly improve your ability to monitor and block any unwanted activity. Modern remote support tools allow technicians to access nearly any type of system or platform, so there is really no need for individual point solutions. By requiring third parties to use your tool for remote access versus their own, it puts you back in control of your company’s security.

2. SHUT OFF ALL OTHER REMOTE ACCESS
The full security value of Step 1 relies on Step 2. Once you’ve chosen an approved remote access tool, block access from any unapproved tools. For example, you can eliminate the need for direct Remote Desktop Protocol (RDP) connections and block broad access to RDP Port 3389, which is a common target for hackers.

You can also block web-based remote access tools that are commonly used by vendors looking for an inexpensive, yet often unsecured, way to access your systems. Simply block all access to those tools from your network.

The free versions of these web-based tools are also often used by tech support call scammers, so blocking them gives you a security bonus should one of your employees be targeted with this type of scam.
3. ELIMINATE SHARED CREDENTIALS AND ENFORCE MULTI-FACTOR AUTHENTICATION

According to Verizon's 2013 Data Breach Investigation Report\(^2\), "76 percent of network intrusions exploited weak or stolen credentials."

Since vendors don't need constant access to your network, they often use one remote access tool license and share generic logins and passwords across technicians. This not only makes the credentials easy for hackers to guess, it means the vendor's ex-employees can often still remotely access your systems.

The best way to protect your network is to require each individual who accesses your network to use unique credentials and two-factor authentication. To do this in a cost-effective way, you'll need a remote access tool that allows vendors to use shared licenses, while still requiring each technician to use a unique username and password.

The next step is to require that every individual uses two-factor authentication to login to the remote access tool. This will not only make it harder for a hacker to use stolen vendor credentials, but also improve compliance with regulations such as PCI-DSS and HIPAA.

4. EMPLOY GRANULAR PERMISSIONS

Most of your vendors only need access to one or a small group of systems on your network. And even then, they may not need full-time access to those systems. So why give it to them? Choose a remote support tool that includes permission settings by vendor or team so you can decide who can access what, and when. When the remote access tool third parties are using is in your control, it enables you to change permissions or cut off access at any time.

5. CAPTURE A SECURE AUDIT TRAIL AND SET UP ALERTS

Most companies don't know they've been hacked until quite a while after the incident. According to the Verizon report\(^2\), “the majority of breaches take months or more to discover.” Think of all the damage a hacker or disgruntled vendor could do over months or even weeks.

That's why it's imperative that your remote access tool captures a secure audit trail of every action your vendor executes on your systems, and ties that record to the unique credentials of the individual user. And make sure the audit trail is captured in a secure place within your own network – not the vendor’s. If they make a mistake, you don't want them to have the ability to delete or modify the record.

---

**BOMGAR FOR SECURE THIRD-PARTY ACCESS**

Bomgar’s Secure Third-Party Vendor Access technology makes it easy to follow the five steps above. By routing all vendor activity through our secure appliance, you can greatly reduce your chance of being the next big data breach victim. Plus, third-party access is built into Bomgar’s core solution so you only have to buy one remote access product for both internal staff and external vendors.

The Bomgar appliance acts as a centralized proxy for vendor activity throughout your enterprise, without the need to deploy hardware to every network segment. Bomgar features include:

- **Embassy Vendor Access:** Bomgar’s Embassy feature is a way to provide secure, auditable, cross-platform remote access to vendors who need regular access to your systems. You can create an Embassy for each and every vendor, and granularly control what systems they can directly access. Creating Embassy teams is a much more secure and manageable alternative to giving third parties VPN access to your internal systems.

- **Single Sign On and Multi-Factor Authentication:** Bomgar supports Kerberos integration for Single Sign On and RADIUS integration for multi-factor authentication using RSA secure ID or other RADIUS authentication providers.

---

- **Granular Access Permissions**: Bomgar includes more than 75 permission settings, so you can fine tune how third parties interact with your systems. For instance, you can disable specific support functions like file transfer and full screen control.

- **Session Recording**: With Bomgar’s video session recording, you can track every vendor action within a remote support session, including who is controlling the mouse and keyboard at any given time during the session. All recordings are stored for up to 90 days on your secure Bomgar appliance, and you can export session videos to external storage.

- **Monitoring & Reporting**: Bomgar captures a full audit trail of all remote support activity and enables you to monitor remote access sessions in real time. You can also set up automated alerts based on system activity, such as if a vendor logs in after hours.

For more information about how Bomgar can help you secure vendor access, please visit: www.bomgar.com/solutions/business-needs/vendor-access.

---

### 9/11 MEMORIAL

“We have numerous vendors that need access to their business systems 24/7 to update them and keep them running. We wanted to make sure that these vendors could remotely access their systems without a lot of difficulty, but at the same time, we wanted the ability to control and monitor access. With Bomgar’s Embassy feature, we were able to do just that. Bomgar was the only solution that met all of our requirements, particularly when it came to security.”

**STEPHEN HAY**

Manager of Technology Infrastructure & Security, 9/11 Memorial

---

“When getting support from a vendor, such as our payroll system provider, the traditional approach was for them to ask us to connect to a WebEx or some other third-party tool. We take a security risk when giving someone outside our network access to our environment. Now, we make them log in with Bomgar, and I can control what they can and can’t do and know that their application will uninstall whenever the session is closed. This is another huge advantage.”

**MIKE CASTILLO**

Director of Network Infrastructure

Eat’n Park Hospitality Group