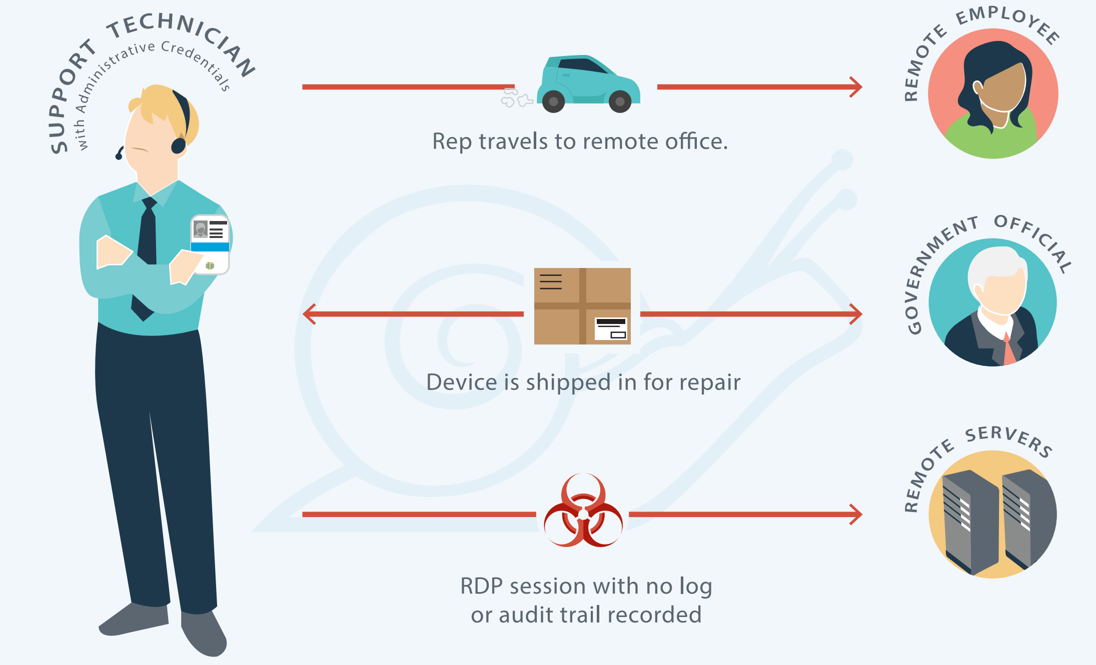
THE SMART CARD DILEMMA

Service Desks and other Support Representatives in government agencies are responsible for supporting employees scattered across the globe, and whether they are just down the hall or across the world, the most efficient way to support them is using a remote support tool.

BEFORE BOMGAR

The enforcement of smart card authentication (including PIV/CAC) in highly secure environments has increased the complexity of providing support. This type of enforcement removes the ability for support technicians to perform administrative tasks on remote workstations, requiring them to travel to that workstation or use other means that can introduce security risks into the environment.



Rep travels to remote office.

Device is shipped in for repair

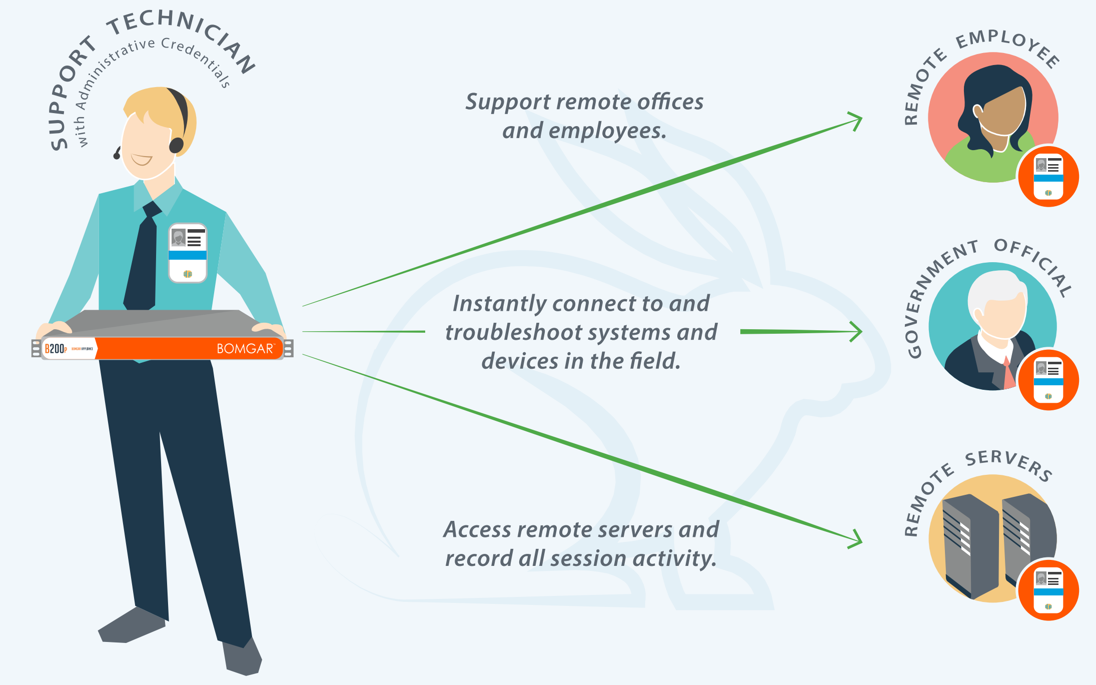
RDP session with no log or audit trail recorded

TIME RESOLUTION: DAYS. POOR PRODUCTIVITY. LITTLE CONTROL

WITH BOMGAR'S SMART CARD SUPPORT

Support technicians can redirect the locally attached smart card (PIV / CAC) to the remote system or device being supported. Technicians can use elevated credentials stored on their local smart card and perform administrative tasks without being at the actual device.

All activity is recorded and logged within the hardened Bomgar Appliance, helping organizations meet strict compliance regulations.



Support remote offices and employees.

Instantly connect to and troubleshoot systems and devices in the field.

Access remote servers and record all session activity.

TIME RESOLUTION: MINUTES. INCREASE PRODUCTIVITY. GAIN CONTROL

SMARTER REMOTE ACCESS *for* SMART CARDS

Bomgar allows you to map PIV and CAC card credentials to remote systems to elevate credentials, improving support efficiency and satisfaction.

IN THE BEGINNING

The push for Smart Card (PIV and CAC) deployment for government entities first began in the early 2000's. More than a decade later, implementation has been a slow process and Smart Cards still have not been adopted across all agencies. In the wake of recent high-profile breaches, there has been a push, or sprint, to improve security across government organizations. One of the projects on the top of every agency's list is full PIV/CAC card implementation.

COMPREHENSIVE SECURITY

Some remote access tools, such as RDP, allow technicians to pass their admin credentials onto the remote device, but they lack the ability to capture a comprehensive audit log of the technician's activity; greatly undermining the security benefits of multi-factor authentication.

OVERCOMING OBSTACLES

A major obstacle of full Smart Card deployment is that the majority of remote support tools are not compatible with Smart Card technology. During a support session, a support representative may need to access a remote system or computer with administrative rights in order to effectively troubleshoot. If a Smart Card is required for authentication, the technician cannot login with their administrative credentials unless they have physical access to the device.

WHAT WE HAVE TO OFFER

Bomgar's Smart Card Support enables government organizations to implement PIV and CAC technology without sacrificing productivity, user experience or security. With Bomgar, agencies can strengthen their security posture while meeting stringent requirements around remote computer and server access.

- ✓ Pass administrative credentials to a remote computer
- ✓ Gain access to remote devices requiring administrative credentials
- ✓ Granularly control session parameters and capture thorough logs of activity done within the session to support monitoring and auditing activities
- ✓ Effectively troubleshoot problems using remote access with tools such as chat and annotation.
- ✓ Satisfy compliance mandates including HIPAA, CJIS, and PCI
- ✓ All transmitted data is encrypted using FIPS 140-2 validated encryption modules. Furthermore, Bomgar also has FIPS 140-2 Level 2 validated options available.