PRIVILEGED ACCESS MANAGEMENT FOR CJIS COMPLIANCE

BOMGAR™

PRIVILEGED ACCESS MANAGEMENT FOR CJIS COMPLIANCE

In 2011, the Criminal Justice Information Services (CJIS) enacted the Advanced Authentication provision, a compliance mandate that set forth minimum security requirements for accessing data within agency systems, including personally identifiable information (PII) such as fingerprint records and criminal histories. The policy went into full effect in September 2013, and now auditors across many states are enforcing these regulations among IT organizations and companies who provide tech support and services to law enforcement agencies.

Many of these auditors have found that the remote access tools used to provide privileged level access to systems and applications in the field do not meet CJIS requirements as most of the solutions offered today do not take a holistic enough approach to managing privileged access.

SECTION 5.5.1 OF THE CJIS POLICY STATES: "The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges."

Misuse of privileged accounts has been a factor in the majority of recent cyber breaches. Cyber criminals are persistently looking for footholds into companies or government networks that are both public and private. Access pathways, such as VPN, can be compromised without the attacker initially having any privileged credentials, allowing them to go unnoticed within the network for weeks or months, allowing them to methodically hunt for a privileged credential to leverage in an attack.

Hackers regularly target privileged accounts because they are aware of the challenge to properly manage the many thousands of privileged accounts commonly found in an organization. Often times, these privileged accounts are shared, unsecurely stored, and give users much more access than they truly need.

SECTION 5.5.6 OF THE CJIS POLICY HAS A FOCUS ON CONTROLLING ACCESS TO SYSTEMS AND STATES: "The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet)."

Security threats through remote access tools are not unique to law enforcement agencies. Legacy point-to-point remote access tools (e.g. RDP, VNC) typically don't offer the access controls and monitoring features required to pass a CJIS audit. They do not allow administrators to set granular parameters for access, nor is it easy to track and record what is happening in a session.

According to the 2018 Privileged Access Threat Report, 62% of respondents lack confidence that they can track vendors with privileged access to their systems. As the complex network of suppliers and third-party vendors within your organization grows, so too does the risk and need for proper policies for the control and management of remote acccess to your network.

"62 percent of respondents lack confidence that they can track vendors with privileged access to systems."

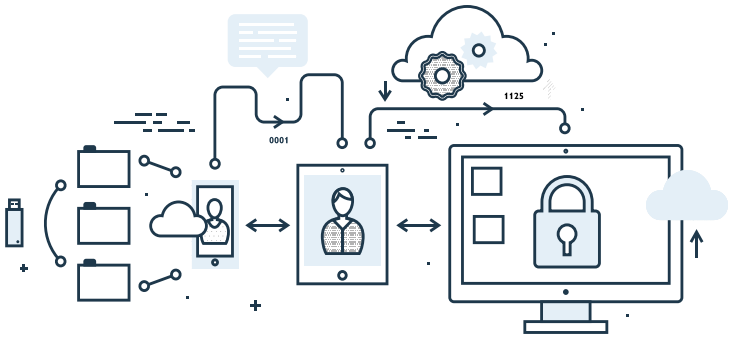
- 2018 PRIVILEGED ACCESS THREAT REPORT

SECTION 5.6.2.2 DEALS WITH ADVANCED AUTHENTICATION AND STATES: "Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.)."

In their September 7, 2016 report on the Office of Personal Management (OPM) breach, The Committee on Oversight and Government Reforming also highlighted the importance of advanced authentication methods. According to the report, "The lax state of OPM's information security left the agency's information systems exposed for any experienced hacker to infiltrate and compromise."

Aligned with CJIS requirements in section 5.6.2.2, one of the primary findings of the House Oversite Committee was the full implementation of basic and required security controls, including multi factor authentication, could plausibly have prevented the breach.

How can organizations efficiently support law enforcement systems in the field while maintaining security and CJIS compliance with respect to Access Control, Least Privilege and Remote Access, and Identification and Authentication?



WITH BOMGAR, YOU CAN MANAGE ALL THE ACCESS TO YOUR NETWORK WITH ONE SOLUTION

Bomgar's Privileged Access Management solution enables security professionals to control, monitor, and manage access to critical systems by privileged users. Bomgar Privileged Access integrates seamlessly with Bomgar Privileged Identity for a true defense in depth strategy that also enhances productivity and meets compliance requirements.

BOMGAR PRIVILEGED ACCESS: Provides administrators, vendors, and business users with the access capabilities they need to be more productive, while protecting high value infrastructure, assets, and applications from cyber breaches.

BOMGAR PRIVILEGED IDENTITY: Continuous, automated account discovery protects privileged credentials at scale. Delegate access to privileged credentials so that only appropriate personnel can log into critical systems and infrastructure.

IMPROVE CYBERSECURITY AND COMPLIANCE

Bomgar Privileged Access resides within your own environment, enabling support for closed networks without compromising security measures. This allows organizations to meet the CJIS requirement to authorize, monitor and control all methods of privileged access.

- **ARCHITECTURE:** Centralized, security-hardened appliance never passes data through a third-party
- **USER AUTHENTICATION:** Integrates with existing identity management and authentication methods, including Smart Cards (CAC/PIV)
- **ACCESS CONTROLS:** 50+ permissions can be assigned individually or through group policies for privileged users & IT vendors
- **AUDIT:** Full audit trail and video recording of session events
- **TWO FACTOR AUTHENTICATION:** Easy-to-use tokenless 2FA
- **CREDENTIAL MANAGEMENT:** Discover, store, rotate, and inject credentials without exposing them to users

> "With the addition of Bomgar Privileged Access Management, I can more efficiently manage our vendors and support reps as seperate entities, but with consistent technology. This addition was seamless for us. ***Bomgar just works, all the time.***"

SCOTT PEPE, TECHNICAL SUPPORT MANAGER

BOMGAR & LAW ENFORCEMENT: A PERFECT FIT

NO OTHER PRIVILEGED ACCESS MANAGEMENT SOLUTION is more tailored to meet the needs of law enforcement agencies than Bomgar. With a cost effective licensing model and load-balanced multi-appliance architecture capable of supporting up to tens of thousands of critical systems, Bomgar is the ideal choice for large, geographically dispersed environments. Bomgar enables you to:

- **IMPROVE** cybersecurity by closing the door on the #1 attack pathway for hackers
- **REPLACE** multiple ineffective remote access tools with a single, comprehensive solution
- **INCREASE** productivity by ditching excel sheets and sticky notes for credential injection
- **STANDARDIZE** the authentication process by adding tokenless 2FA and integrating with Smart Cards and external directories
- **SECURE** access across hybrid environments to support existing IT infrastructure
- **SIMPLIFY** regulatory compliance
- **IMPLEMENT** a solution your users will love

ABOUT BOMGAR

Bomgar is the leader in Secure Access solutions that empower businesses. Bomgar's leading remote support, privileged access management, and identity management solutions help support and security professionals improve productivity and security by enabling secure, controlled connections to any system or device, anywhere in the world. More than 13,000 organizations across 80 countries use Bomgar to deliver superior support services and reduce threats to valuable data and systems. Bomgar is privately held with offices in Atlanta, Jackson, Washington D.C., Frankfurt, London, Paris, and Singapore. Connect with Bomgar at www.bomgar.com.

CONTACT | INFO@BOMGAR.COM | 866-205-3650 (U.S.) | +44 (0)1628-480-210 (U.K./EMEA) | BOMGAR.COM