Protect Your Endpoint Data: Mitigating Threats with Cigent Data Protection

#1. INTRODUCTION

Despite investments in networks and endpoints, attackers continue to compromise sensitive data. From ransomware-as-a-service enabling volumes of attacks to data breaches orchestrated by sophisticated hackers, the risks are multiplying, and the stakes have never been higher.

According to a *Verizon study,* 70% of all data losses occur at the endpoint, and with *27 billion endpoint devices* expected to be connected by 2025, the need to protect that data is greater than ever.

As organizations strive to stay ahead of these evolving threats, they must adopt proactive measures to fortify their defenses and safeguard their valuable assets. This is where Cigent steps in.

Cigent shifts the paradigm from detection and response, to protection. By focusing on protecting the data itself, Cigent ensures the integrity of data, stopping malicious data encryption, exfiltration, and tampering even when the device itself has been compromised. Protecting the modern workforce, security solutions must be not only effective and seamless, but also minimize impact on the end user and overburdened endpoint and security teams.

Cigent provides a resilient defense that stands strong against even the most formidable threats, ensuring that your data remains safe, secure, and protected at all times.

#2. UNDERSTANDING THE THREAT LANDSCAPE

Why should you be concerned about your endpoint data? While data has certainly moved into the cloud, sensitive data continues to reside on endpoints. Sensitive data is defined as any sort of data which would cause the need for a data breach notification if it were accessed illegally, from credit card data, to personal information. According to research, sensitive data can be found on *73% of all endpoint devices.* These represent a significant data risk for organizations.

Significant investments have been made in securing vulnerable endpoints. Leveraging AI (artificial intelligence), EDR dramatically improved protection vs legacy antivirus, but cyber attackers continue to innovate and penetrate defenses. *According to a study by the Ponemon Institute,* 68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. Ransomware gangs continue to collect record amounts of money from the organizations they target. The fact is bad actors keep finding a way through, and these attacks are predicted to get worse.

Consider the growing use of AI by cyber attackers. The UK's *National Cyber Security Centre* predicts that AI will almost certainly heighten the volume and impacts of cyber attacks over the next couple of years. They state that all types of cyber threat actors are already using AI as a tool to compromise data protections and AI has lowered the barrier for novice cyber criminals.

Advances in social engineering are also helping bad actors to construct more targeted, elaborate phishing scams. *According to GreatHorn, 57% of organizations experience phishing attempts on a weekly or daily basis.* Malicious actors are using every tool at their disposal to learn what they can about their targets and deliver messaging to draw them in. While this isn't a new technique, AI is enabling attackers to increase the volume and sophistication of these attacks.

As the sophistication and frequency of attacks continue to increase, detection and response will become increasingly insufficient. Security and endpoint teams, even leveraging new capabilities and techniques, will be challenged to effectively address attacks before compromise occurs.

Already vulnerable, AI will be a catalyst for new innovative attacks that will only increase compromises, losses, and disruptions.

Any approach to improve the security posture, must balance the needs of the modern workforce. End user productivity must be balanced with the need to mitigate risks. Restricting access, implementing access controls, or other approaches compromising user experience will likely be met with resistance inhibiting adoption.

In the face of escalating cyber threats, organizations must evolve their detect and respond paradigm and adapt a proactive to protecting endpoint data. At the same time, it's important that usability and efficiency are maintained. In the following sections, we'll explore how Cigent's innovative endpoint data security solutions can help businesses mitigate these risks and stay
ahead of emerging threats.

#3. THE CIGENT SOLUTION

The detect and respond model is insufficient to protect data in the face of increasingly sophisticated attacks. Cigent's approach is proactive security that ensures data remains protected even when a device has been compromised. As the solution is focused on the data itself, it protects against all data threats, including data exfiltration, encryption (i.e. ransomware), destruction, and tampering.

Cigent provides an Endpoint Data Protection Platform that allows organizations to seamlessly scale capabilities to address their data security requirements. The portfolio addresses data at rest protection, protection of data from remote attacks, and even prevention of the most advanced persistent attacks. The Cigent portfolio can enable you to meet a variety of compliance requirements efficiently.

PROTECTING DATA AT REST

Endpoint devices will go missing. *According to Gartner's research, a laptop is stolen every 53 seconds.* The foundation of protection at rest is software or hardware data encryption. Cigent effectively delivers both with management for Microsoft BitLocker delivering software encryption, and Solid State Drives for more secure hardware-based encryption.

Microsoft BitLocker encryption enables organizations to meet minimum data-at-rest security standards. Encrypting data at the OS level will prevent unsophisticated actors from accessing data on a lost or stolen device. Cigent BitLocker manager was designed to streamline deployment, management, troubleshooting, and reporting to ensure effective deployment with minimal overhead.

Hardware-based encryption with self-encrypting drives significantly increases the protection of data at rest. With the encryption originating from the device firmware level it prevents common tactics inclined passware kits that can circumvent OS-level encryption. For additional security, organizations can utilize pre-boot authentication that provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Devices with Cigent for PBA deployed would defeat all but the most sophisticated attackers.

Organizations requiring even a more secure posture can choose to deploy both BitLocker and SED simultaneously. This approach can address stringent compliance requirements and mitigate the risk of future computing advances, including quantum.

Cigent also offers multiple options for managing your at-rest encryption. Organizations seeking efficient scale will utilize the Cigent cloud management console, while those focusing on risk mitigation can use its command-line interface for direct provisioning of the solution.

Efficient, effective data-at-rest protection.

STOPPING RANSOMWARE AND DATA ATTACKS

Protecting data when a device is used is a far more complex proposition. The paradigm of detection and responding continues to be challenged by the ever-evolving threat landscape. Cigent delivers the industry's first solution that protects endpoint data while the user is active, even if the device is compromised.

Cigent uses layers of protection to prevent malicious data exfiltration, encryption (i.e. ransomware), tampering, or any other data attack. Protection begins with a "trust, but verify" approach, utilizing step-up authentication for file access. This simple but effective approach prevents ransomware or other data attacks from accessing data even after a device is compromised. The policy-driven approach ensures that only authorized users can access data. With granular policy controls and AI-enabled enforcement, user disruption is minimized.

Organizations employing SEDs have the additional capability of partitioned, hidden drives. The capability renders the drives and all data within completely invisible to malware, unauthorized users, or even alternate operating systems. Data is unreadable at the sector level and cannot be cloned or wiped preventing even sophisticated adversaries from compromising your data.

Additionally, Cigent provides additional protection by working with existing endpoint protections, including EDR, SIEM, and SOCs. With automation and integration, Cigent will elevate data protection as these solutions detect potential threats. Cigent continually monitors local EDR agents for a "heartbeat," instantly elevating protection when an adversary has rendered these solutions inoperable. These integrations, coupled with Cigent's own proprietary AI monitoring, further mitigate exposure with only files actively in use at risk of compromise.

Cigent delivers an entirely novel and effective solution to prevent data compromise. With minimal user impact and virtually no IT administration, it prevents attackers from accessing data preventing any malicious compromise. With data protected, users can continue to remain productive during attacks without the need to isolate or disconnect.

ADVANCED AND PERSISTENT THREAT PROTECTION

Sophisticated and persistent attacks, particularly those with physical access, can bypass conventional security measures. Nation-states or sophisticated criminal syndicates can employ a variety of remote or physical attacks to compromise endpoint data. Remote adversaries have already developed polymorphic malware and are embracing AI to develop even more sophisticated techniques. Adversaries with physical access can defeat even SEDs leveraging a variety of methodologies including alternative O/S and drive manipulation.

Cigent was developed by the world-leading experts in data recovery and sanitization who reverse-engineered their approach to develop the most secure endpoint capability. The solution is embedded with firmware providing protection to thwart the most advanced adversary.

Data is protected at rest with inaccessible encryption keys. Creation and storage of keys use a proven methodology that prevents recreation or retrieval. At rest, data is also protected by drives that, with PBA, render the O/S partition invisible.

Cigent also employs unique AI monitoring with embedded AI microprocessors that continuously monitor data activity. While other endpoint solutions use AI to evaluate application behavior, Cigent monitors data access patterns automatically, activating protective measures when ransomware-like activity is detected. AI also monitors for physical tampering locking data. With the AI embedded within the drive, it is impervious to compromise.

Cigent provides organizations seeking to protect the integrity of sensitive data against the most sophisticated adversaries with uncompromising security without compromising user experience or requiring significant administrative overhead.

ADDRESSING COMPLIANCE MANDATES

Cigent enables organizations to meet compliance requirements for a myriad of vertical and risk postures. This includes common compliance requirements including FIPS 140-2, NIST 800-171, CMMC, GDPR, HIPAA, CCPA, and EO14028. In addition, Cigent enabled drives meet CSfC for data at rest NSA mandates.

Cigent enables organizations to not only meet their compliance requirements but streamline all aspects of the solution administration. Organizations can administer at scale through a modern cloud console that has been optimized for reporting. Whether meeting audit compliance or dealing with an event, Cigent efficiently collects and reports data on your endpoints. For organizations with security requirements prohibiting cloud access, Cigent offers a command line interface that provides documentation for compliance requirements, as well as an on-prem installation available.

Cigent is unique in the breadth and depth of its offerings to enable organizations to meet compliance requirements. With its cloud console, administrators have a single console to meet various mandates across their portfolio.

#4. KEY BENEFITS OF CHOOSING CIGENT

Cigent solutions are unique in their singular focus on protecting the data itself. With this approach to safeguarding your organization's sensitive data against the cyber threats, Cigent stands apart with our innovative "Four Protects."

1. PROTECTS EVEN WHEN THE DEVICE IS COMPROMISED.

Cigent goes beyond traditional security measures to safeguard your data, even in the event of a compromised device. How do we achieve this? By employing advanced techniques such as hiding data in undetectable drives and implementing zero-trust access controls that limit exposure to unauthorized users or malware.

2. PROTECTS AGAINST ALL FORMS OF ATTACKS.

Whether facing physical intrusion or remote cyber-attacks, Cigent provides comprehensive protection within a single solution. A single solution can ensure the integrity of data regardless of the threat vector and approach. Cigent accomplishes this mission with layers of data protection using a combination of proven approaches and patented innovative capabilities. Zero-trust access controls, protected drive, and AI enforcement provide complementary protection preventing data compromise.

3. PROTECTS DATA WITH MINIMAL USER IMPACT.

Designed to protect the modern workforce, the Cigent solution maintains data protection without disrupting end-user productivity. Most of the protection capabilities are transparent to the end user. Zero-trust access controls and granular policy controls allow organizations to align authentication requirements with security posture. Enabled by AI optimization that continually assesses and adjusts security measures, end users' disruptions are minimized while ensuring protections. And by protecting the data itself users can remain productive even after a successful attack.

4. PROTECTS WITHOUT ADMINISTRATIVE OVERSIGHT.

The detect and respond paradigm requires constant oversight and remediation. Cigent proactive approach delivers "set and forget" protection. Data that is not actively used is always protected. Cigent further mitigates risk through integration and automation with EDR solutions and employs its own AI to elevate protections when threats are elevated or an attack has been detected. Endpoint and security teams can be confident that your data is safeguarded without continually responding to threats. The Cigent cloud console was designed to streamline tasks enabling efficient administration and reporting for when your data is at rest or in use.

#4. CIGENT'S CAPABILITIES

Cigent's effectiveness is due to its layered capabilities, which build off one another to prevent compromise from any threat. Cigent capabilities include:

- **Zero-trust access control:**
Ensures that only authorized users can access sensitive files, preventing unauthorized access and data breaches. Granular policy controls align risk with persona, and AI-supported controls minimize end-user impact while maintaining a security posture.

- **Hidden Drives:**
Cigent's hidden drives render data completely invisible to malware and unauthorized users until unlocked with step-up authentication. This set-and-forget capability requires no overhead for IT administrators, providing seamless protection against remote or physical attacks.

- **Automated Threat Response:**
Cigent enhances existing protections through integration with EDR, SIEM, and SOC solutions. As these solutions elevate their threat level, Cigent increases protection to minimize exposure. In addition, as a common tactic of attackers is to render local security agents inoperable, Cigient monitors for a “heartbeat.” Upon detection that the EDR has been compromised, Cigent immediately elevates protection.

- **Inaccessible Keys** *(available on Cigent drives):*
Encryption protections are only secure if adversaries cannot recreate or access keys. Cigent uses a proven methodology for the creation and storage of keys rendering all known compromise approaches nearly obsolete. Keys are created using the maximum number of characters allowed with a technique that prevents replication. Once created, keys are deconstructed and distributed across the drive eliminating
the risk of attackers discovering key locations.

- **AI Protected Storage** *(available on Cigent SSD+ drives):*
Cigent uses proprietary AI that monitors data access patterns for anomalous behavior. This approach ensures that even a sophisticated threat actor will be discovered with instant automation locking all drives and data. In addition, the AI is embedded within storage, making it inaccessible to tampering.

- **Verified Data Erasure** *(available on Cigent drives):*

Sophisticated actors have developed techniques to retrieve data from drives that have been deleted or destroyed using conventional methods. Cigent patented technology ensures that data has been permanently erased. The solution performs a crypto wipe followed by a full block-level wipe. It then verifies at the block that each block has been wiped. Organizations can issue erasure commands remotely or on
the device. The approach allows for drives to be safely repurposed or recycled versus expensive and wasteful destruction methodologies.

- **Secured Data Logs** *(available on Cigent drives):*

Cigent tracks and documents all data activity. It creates immutable log of data activity that cannot be altered, amended, or deleted preventing external attackers or insiders from “covering their tracks.” Only solution that tracks data when insider boot from USB stick.

Cigent empowers organizations to protect their valuable data assets and defend against the evolving threat landscape effectively. With Cigent, organizations can achieve peace of mind knowing that their data is secure, compliant, and resilient in the face of cyber threats, even where devices have been compromised.

#5. CONCLUSION

Endpoints are critical tools for organizations and will continue to be a source for the creation, manipulation, and storage of sensitive data. Existing protections are insufficient to ensure data remains protected, and with adversaries embracing AI, attacks will only increase in volume and sophistication. More attacks will be successful, more data will be compromised, and more organizations will face significant disruption and costs.

Cigent resets endpoint data protection paradigm from detect and respond to proactive protection. By protecting the data itself Cigent is able to protects data from physical or remote attacks even when the device is compromised. protects with minimal user impact, and protects with virtually no administrative overhead.

Utilizing proven approaches, new methodologies, and patented technologies, Cigent's layered approach provides unparalleled protection with minimal user impact and administrative oversight. The solution empowers organizations to defend against emerging threats, ensure compliance with regulatory requirements, and preserve the trust and confidence of customers and stakeholders.

Experience the difference with Cigent and take proactive steps to secure the future of your business in an age of uncertainty. Together, we can navigate the challenges of the digital world and build a resilient defense that stands strong against even the most formidable adversaries.

Don't just detect cyber threats, protect your endpoint data with confidence.

GETTING STARTED WITH CIGENT

Take the First Step Towards Endpoint Data Security with Cigent
Ready to fortify your organization's defenses against cyber threats and safeguard your valuable data assets? Don't wait until it's too late. Take the first step towards comprehensive endpoint data security with Cigent today.

Contact us now to schedule a demo and discover how Cigent can help safeguard the future of your business. Together, we'll build a resilient defense that stands strong against cyber threats and ensures the resilience of your business.

Take action now. Choose Cigent and protect what matters most.

ABOUT CIGENT

Cigent offers leading-edge data security solutions for endpoint devices built on the premise of offering a more secure approach to data protection. Where traditional approaches follow a reactionary "detect and respond" strategy, Cigent proactively uses multiple layers of protection for data. This means that even if the device itself is compromised, the data will be kept safe.

Funded by In-Q-Tel, Cigent continues to protect valuable data assets against all forms of attacks. Our team is committed to innovation, keeping your data protected while minimizing impact on the end user experience. We hold various NIST, NIAP, and NSA certifications, which are used by multiple federal agencies in the United States