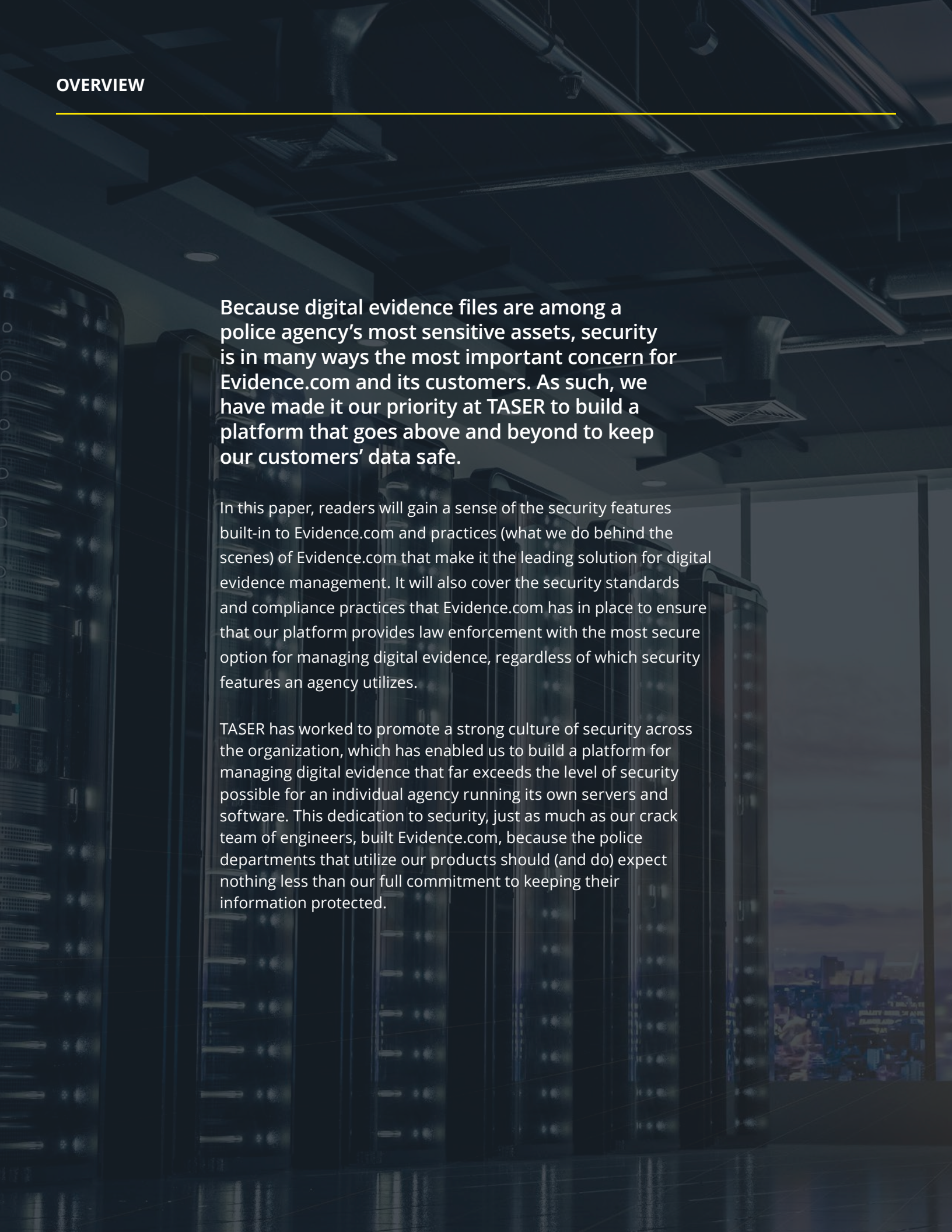
TASER | AXON

BEYOND CJIS:
ENHANCED SECURITY, NOT JUST COMPLIANCE

PROTECT LIFE.
PROTECT TRUTH.

OVERVIEW



Because digital evidence files are among a police agency's most sensitive assets, security is in many ways the most important concern for Evidence.com and its customers. As such, we have made it our priority at TASER to build a platform that goes above and beyond to keep our customers' data safe.

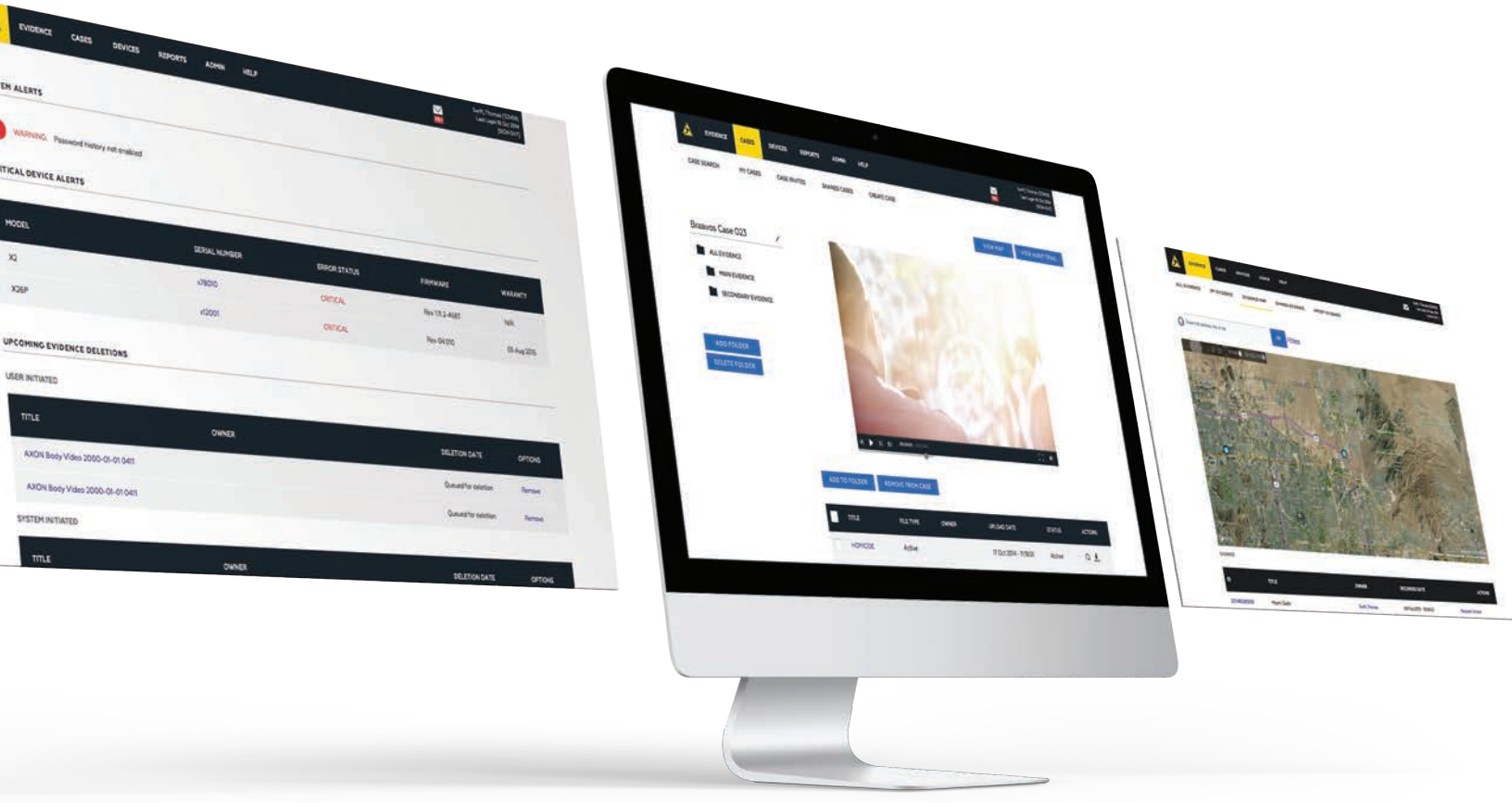
In this paper, readers will gain a sense of the security features built-in to Evidence.com and practices (what we do behind the scenes) of Evidence.com that make it the leading solution for digital evidence management. It will also cover the security standards and compliance practices that Evidence.com has in place to ensure that our platform provides law enforcement with the most secure option for managing digital evidence, regardless of which security features an agency utilizes.

TASER has worked to promote a strong culture of security across the organization, which has enabled us to build a platform for managing digital evidence that far exceeds the level of security possible for an individual agency running its own servers and software. This dedication to security, just as much as our crack team of engineers, built Evidence.com, because the police departments that utilize our products should (and do) expect nothing less than our full commitment to keeping their information protected.

Part of the Axon platform, Evidence.com is a tool for managing digital evidence from capture to courtroom.

Built for compatibility with our increasingly widely adopted Axon cameras, this system is designed to ingest, process, and store evidence files in the cloud. It is easy to use and allows for more streamlined collaboration within departments as well as outside of them.

Agencies retain all ownership of their files, but by storing them in the cloud they can alleviate many of the costs of on-site data storage while (we contend) reducing their level of vulnerability. But what features does it have for keeping your data safe?



Our first priority whenever we create new hardware or software is security.

Because we have more than two decades of experience working with law enforcement, we are able to draw from a comprehensive view of the unique security needs that come with the sensitive nature of police work. Our focus on security means that our Evidence.com cloud platform boasts an array of security features designed to protect evidence files for tampering and unauthorized access and are available within the application itself.

ACCESS CONTROL:

Our approach to security features 'built' in to Evidence.com begins with providing users with robust access control options. Because the agencies we work with deal with varying levels of risk, we offer customization in terms of password length-and-complexity requirements and failed login limits. By default, we enforce a strong baseline built on best practices.

For instance, our system features forced session timeouts, mandatory challenge questions when users first authenticate from a new location, and multi-factor authentication options. This means that even if someone has stolen a user's ID and password, he or she is still unlikely to be able to access Evidence.com.

While these features safeguard against potential attackers gaining access to some part of the system from the outside, we also take care to ensure that users within the system are only able to access what is strictly necessary. This starts with role-based permissions, and continues into device-based permissions, which let an agency restrict the use of the interface to certain devices (i.e., enabling officers to access data through the web-based platform but not through the mobile application), and IP address restrictions. We also integrate with agency's directory services, to streamline account provisioning and management. Not only is chain of custody maintained, but the likelihood of an attacker tampering with evidence is greatly decreased, since an attacker is highly unlikely to access any evidence in the first place.

EVIDENCE.COM APPLICATION SECURITY FEATURES

EVIDENCE INTEGRITY:

Built for law enforcement, Evidence.com is uniquely sensitive to the needs that surround the handling of evidence. For instance, automatic audit trails keep a complete and unalterable log of who has uploaded, accessed, edited, or shared each evidence file and when, in order to ensure that the proper chain of custody is maintained. As with physical evidence, however, there is more to protecting the integrity of data than audit trails. Data hashing, for example, is employed to create a forensic fingerprint of each file, which is validated before and after evidence transmission to ensure that the evidence hasn't been compromised.

These forensic fingerprints can be used later to unequivocally prove that evidence is authentic and free from tampering. Once evidence is uploaded, the original file is never altered. When a user edits a video or creates a clip or a redaction, their work is saved as a new, separate file. When a user does want to delete a file, there is a seven-day grace period during which your evidence can be retrieved if it was wrongly deleted.

Forensic fingerprint of each evidence file using industry standard SHA hash function. Integrity is validated before and after upload to ensure no changes occurred during transmission.

Full tamper-proof evidence audit records. Logs the when, who, and what for each evidence file. These records cannot be edited or changed, even by account administrators.

Original evidence files are never altered, even when derivative works (video segments) are created.

Deletion protection, including deletion approval workflows, deletions notification emails, and a deletion remorse period to recover accidentally deleted evidence files.

We've built a platform that incorporates everything we know about making data available only to those who should have access to it, but that doesn't mean that our job is finished.

The continued success of Evidence.com is built upon ongoing, day-to-day operations designed to keep us as many steps ahead of any would-be attackers as possible. This encompasses not just regular security audits and the like, but also our hiring practices and evolving partnerships with cloud infrastructure providers.

ENCRYPTION

Encryption is one of the keys to ensuring the safety of data both when it's stored and as it's being transferred, which is why we aim for encryptions that are as robust as possible. Specifically, we have implemented Transport Layer Security (TLS) with a RSA 2048-bit key and a 256- or 128-bit connection (depending on client browser) when your data is in transit and 256-bit Advanced Encryption Standard (AES-256) when your data is being stored.

ADVANCED PROTECTIONS

By having a laser focus on security and aggressively investing to maintain such security, we are able to deploy and appropriately manage advanced security tools and threat prevention solutions that are cost- or resource-prohibitive to individual agencies. Unlike what you would find with an off-the-shelf anti-virus software that you install yourself, we offer advanced protections that deter even the most sophisticated attackers. We have finely tuned web application firewalls, leverage security intelligence tools for continuous monitoring, and deploy layers of defense to detect and react to any malicious activity.

MONITORING

Though it typically requires a sizable support staff, early detection can be a significant factor in minimizing the effects of, and outright preventing, malicious activity. To identify and halt any potential breaches of the system as quickly as possible, security professionals well-versed in the ways that attackers might try to find and exploit vulnerabilities monitor Evidence.com around the clock. If any suspicious activities are detected, our team has a set of protocols in place designed to mitigate any potential ill effects of an incident. We immediately notify the appropriate parties and maintain a careful record of the incident to inform our future security updates and patches.

PERSONNEL

Because TASER is fully aware that we are handling agencies' most sensitive assets, hiring security-conscious people to work on Evidence.com is an absolute must. This begins with criminal background checks for all potential hires, and continues with mandatory security training at least each year for all employees. This ensures that even members of our team who won't be working on Evidence.com directly understand that the real security of your stored data begins with our own practices within the company.

When it comes to our Evidence.com team in particular, we make a point of hiring talented security professionals with experience protecting critical information. Even the most security-conscious agency would be unlikely to produce a team that rivaled ours for resources and know-how.

AXON PLATFORM SECURITY FEATURES

SECURITY AUDITS

In addition to constantly monitoring for the presence of attackers and to adapt our system to the latest attacks, TASER's security team oversees regular vulnerability scans and penetration tests. Because our team has the resources and resourcefulness to stay on the cutting edge, they are constantly searching for new and creative ways that the system might be compromised, so preventative measures can be taken as needed.

Not only do frequent security audits greatly increase the likelihood that we'll find vulnerabilities before any attackers have the chance, they also incentivize the frequent software updates that are crucial to keeping your information safe. In fact, running out-of-date software is one of the most significant security risks faced by agencies utilizing local software. Evidence.com's automatic, system-wide software updates are functionally a security feature in and of themselves.

PARTNERSHIPS

Beyond its own dedicated security team, Evidence.com builds the foundations of its security framework on the features and best practices of our Infrasturcture as a Service (IaaS) providers.

TASER has partnered with industry-leading Infrastructure as a Service providers to deploy a secure, extremely scalable and highly reliable infrastructure to operate Evidence.com. This partnership includes a shared commitment to ensure the infrastructure operating Evidence.com is aligned with the CJIS Security Policy. Additionally, TASER's IaaS providers comply with many security assurance and certification programs and undergoes regular security audits. These include SOC 1/SSAE 16, SOC 2 & 3, CJIS, ISO 27001, FedRAMP, PCI, FISMA, and FIPS 140-2. TASER International regularly reviews the specific security practices and audit results documented by our IaaS providers to ensure the highest standards are met.

PHYSICAL PROTECTION

Just as we make a point of implementing strict access control on the system itself, we and our IaaS vendors employ an equally strict system for managing the physical locations where your data is stored. Our vendors offer nondescript storage facilities whose access is monitored diligently at all times by a team of professionals utilizing video surveillance and intrusion detection systems. Data center floors can be accessed only by those with a legitimate business objective (and only after they have passed two-factor authentication at least twice), and access is immediately revoked once said objective is no longer applicable. This ensures that we adhere to a principal of "least privilege," which helps to minimize the risk of compromise.

Just as all activity in Evidence.com is tracked with an unalterable audit trail, these data centers keep precise logs of all physical access. TASER audits these logs in the course of our vendor security evaluations, which are undertaken regularly to ensure that our exacting compliance expectations are being met.

Though this whitepaper has taken pains to outline the robust nature of our security processes, we can't expect everyone to take our word for it.

That's why we strive to work within existing security policies and have sought out certifications from third parties.

Not only is Evidence.com compliant with the FBI's CJIS security policies, but it actually exceeds its requirements. The CJIS policy addresses factors like access control and encryptions that have been laid out above, as well as audit trails and criminal background checks for personnel. Evidence.com is designed to easily pass a CJIS audit and TASER's information security team can be made available to agencies who need assistance with a potential audit.

In addition to being CJIS compliant, Evidence.com is ISO/IEC 27001:2013 certified, which means that third parties have affirmed the robust nature of our organizational commitment to constantly-evolving information security practices.

Beyond our outside certifications, TASER maintains a seven-figure cyber security insurance policy that insures against a breach of Evidence.com. Our customers can join this policy for added protection.