Improving Data Protection
with
Endpoint Security

CERVAIS WHITE PAPER

Author: Dr. James Andrew Austin

Introduction

Mobile devices continue to be the target of attack at increasing rates. There is a relatively simple explanation for this - in a typical organization today, 60% of the endpoints containing or accessing enterprise data are mobile; the majority of which do not have any security protection today. It is no longer a matter of if or when an enterprise's mobile endpoints or even consumer devices are at risk--they already are. Mobile devices contain or have access to the same information as traditional endpoints.

While billions of dollars have been spent protecting and securing traditional endpoints, very little has been invested to protect mobile device endpoints. Attackers work on the same model as any other business: where do they get the greatest return on their investment of time and resources. As a result, mobile devices have become a favorite attack target and that trend is not likely to decrease any time soon. As connected devices expand, the attack vector grows larger and possibly less detectable.

Generally speaking, data protection measures resist internal and external disruptions and attacks on critical data and endpoint devices at large. These measures are applied over the entire lifecycle of the data from when the data is generated to when the data is destroyed or securely archived. Applying suitable measures to data-in-use, data-at-rest and data-in-motion, encourages confidence in the security protections of the endpoint device.

Failure to apply proper data protection measures can lead to serious consequences for endpoint devices, such as:

- Theft of Information
- Loss of Integrity
- Loss of Confidentiality
- Loss of IP, and negative impact on brand reputation
- Disrupted Communications
- Loss of Privacy

The Importance of Endpoint Security

As the Internet continues to go mobile, smart devices such as those used for home automation, smartphones, tablets, security cameras, baby monitors and Internet of Things (IoT) devices have become prime targets for cyber-attacks; the threat is real. But how much do consumers know about the risk of mobile security threats? Do they protect their mobile devices from online threats? Have they been victimized by a cyber-attack? Who do they call for help during or after a cyber-attack?

According to a study conducted by Attot Communications, consumers have heard about various types of cyber-attacks and say they protect their device (only a small percentage of around 11%) and few actually pay for protection. The vast majority who do not pay could be using free security apps or security settings on their device which they perceive as providing sufficient protection. Endpoint security aims to adequately secure every endpoint to block access attempts and other risky activity at these points of entry.

Understanding the Real Cost of Data Protection

The mobile computing footprint has exploded. In some parts of the world it has completely surpassed desktop use. According to a report produced by Hootsuite, Sixty-six percent of the world's population now uses a mobile device. Securing all access points and applications across all devices has been almost unachievable until now. With the rise of cyber-attacks against consumers and organizational devices, it can be a difficult task to precisely calculate the cost-to-benefit ratio that mobile security technology provides, but it's easy to imagine what the real-world cost to the mobile device user would be if faced with this situation:

You recently purchased a brand new laptop with all the bells and whistles and also included with your purchase was anti-virus software. Once getting home you install additional software applications and get everything configured just like you want it and then finally connect your new laptop to your home network. A week later you realize that that some of your files are missing and some of the configuration parameters within various applications have been changed from their original settings. Now being concerned about a possible cyber-attack on your home network, you check some of the configuration settings on other devices connected to your home network. Long and behold, you find that other device settings have been changed and you also recognize that some of your passwords are now not working.

It might be tempting to dismiss this hypothetical nightmare scenario as unrealistic or overly paranoid, but the news is full of examples of what happens when people or organizations under invests, or choose a poor security strategy for protecting their endpoint devices. When you consider that mobile and device app developers aren't security experts – many are designers using app development platforms – mobile has become ripe for "cyber a disaster."

Some of the incidents which recently made the headlines include:

- In 2019, researchers from security firm Clever Security discovered that the Conexus Radio Frequency Telemetry Protocol (Medtronic's proprietary means for monitors to wirelessly connect to implanted devices) provides no encryption to secure communications. That makes it possible for attackers within radio range to eavesdrop on the communications. Even worse, the protocol has no means of authentication for legitimate devices to prove they are authorized to take control of the implanted devices. That lack of authentication, combined with a raft of other vulnerabilities, makes it possible for attackers within radio range to completely rewrite the defibrillator firmware, which is rarely seen in exploits that affect medical device vulnerabilities.

- In 2019, Ashley LeMay and Dylan Blakeley recently installed a Ring security camera in the bedroom of their three daughters, giving the Mississippi parents an extra set of eyes — but not the ones that they had bargained for. Four days after mounting the camera to the wall, a built-in speaker started piping the song "Tiptoe Through the Tulips" into the empty bedroom, footage from the device showed. When the couple's 8-year-old daughter, Alyssa, checked on the music and turned on the lights, a man started speaking to her, repeatedly calling her a racial slur and saying he was Santa Claus; she screamed for her mother. The family's Ring security system had been hacked, the family said. The intrusion was part of a recent spate of breaches involving Ring, which is owned by Amazon.

- In 2019, a hacker exploited a security weakness in a set of baby monitors in a Houston couple's home, threatening to kidnap their child. The Houston couple were sleeping downstairs just before midnight while their 4-month-old son, slept in his room upstairs. The couple stated that the beeping from the monitor woke them up and that they initially thought it was just a carbon monoxide alert. However, they heard a voice coming from the monitor, speaking with vulgar language. After the couple got out of bed, and turned on the lights in their room, the second monitor in their bedroom turned on and the voice ordered them to turn the lights off. The man's voice then told the couple that he was in Topper's room and was going to kidnap him. After checking that the child was safe, the couple remembered a story on Wi-Fi hacking that they had read online. The couple just had to figure out how to get the Wi-Fi shut down, and shut down fast. The wife kept telling her husband, "he's not in here, somebody's hacking this."

Intrusion and Theft – Real Possibilities

When determining the type of endpoint protection to utilize for mobile devices, the end user must think about a comprehensive security approach that will address concerns about securing the device's wired and wireless connections. Encryption of data, secure communications, identification, verification and authentication and threat notification measures are necessary. After all, consumers and organizations alike should not buy products unless they know that they will protect their data, services and infrastructure against intrusion, theft and sabotage. Unless properly secured, mobile and IoT devices can become a prime target for interception of sensitive data, theft or other services. Poorly secured communications can also be susceptible to man-in-the-middle attacks and other techniques intended to inject malicious code during routine software upgrades. Once inside your system, the new code can turn the device into a convenient point of entry to other devices within your environment that can be used to gain access to sensitive consumer and corporate data.

Similar techniques can also be utilized by those with more threatening intent to do physical harm. Several Pentagon studies, and recent real-world incidents such as the Flame and Stuxnet viruses, should serve as clear warnings that cyber-terrorism is a real possibility, especially in applications involving public infrastructure (utilities, communication, transportation) or mission critical systems (medical, industrial control, etc.).

Implementing the Right Security

As mentioned in this paper, when selecting an effective security solution for the protection of endpoint devices, the user should consider a solution that provides for the protection of data-in-use, data-at-rest and data-in-motion and encourages confidence in the security protections of the endpoint device. While there are many products on the market that claim that they can provide a level of security protections to the endpoint device that are bullet proof, the fact is these claims cannot be proven.

Threats range from advanced nation state attacks, to organized crime using advanced fraud technologies, to simple theft of mobile devices. The threats to users of mobile devices include, e.g., user location tracking, attackers seeking financial gain through banking fraud, social engineering, ransomware, identity theft, or theft of the device and any sensitive data. Cervais® has developed an innovative way to protect the mobility of this digital movement and is positioned to become the solution of choice when it comes to device data protection.

The rapid evolution of mobile devices and IoT is exciting, but securing them has become a significant challenge for consumers and organizations in every sector. As connected devices proliferate, the attack vector grows larger and possibly less detectable. Cervais is transforming endpoint protection by being the first and only organization to architect an Advanced Endpoint Protection (AEP) system - all delivered via a small and compact mobile solution.

Cervais D-RISK® Mobile Data Protector

Cervais D-RISK® Mobile Data Protector is a portable Cyber security device that provides complete data protection and employs some of the most advanced data forensics detection and monitoring techniques available to combat and detect threats to a user's endpoint device as well as the IoT. As adversaries and their tactics and procedures continue to become more targeted, dynamic, and sophisticated, D-RISK Mobile is positioned to become the solution of choice when it comes device data protection.

Cervais D-RISK Mobile is built around a threat intelligence framework that employs our Inteli-Sense™ Analytics (ISA) engine, the core of which manages an extensive array of artificial intelligence algorithms. With Inteli-Sense, our D-RISK Mobile solution applies predictive analytics to monitor and detect anomalies from all inbound and outbound attack vectors associated with a user's endpoint device—and neutralize any threats. Cervais D-RISK Mobile uses the power of machine learning to identify, locate, authenticate, notify and protect user endpoint devices wherever the user may be, anywhere in the world.

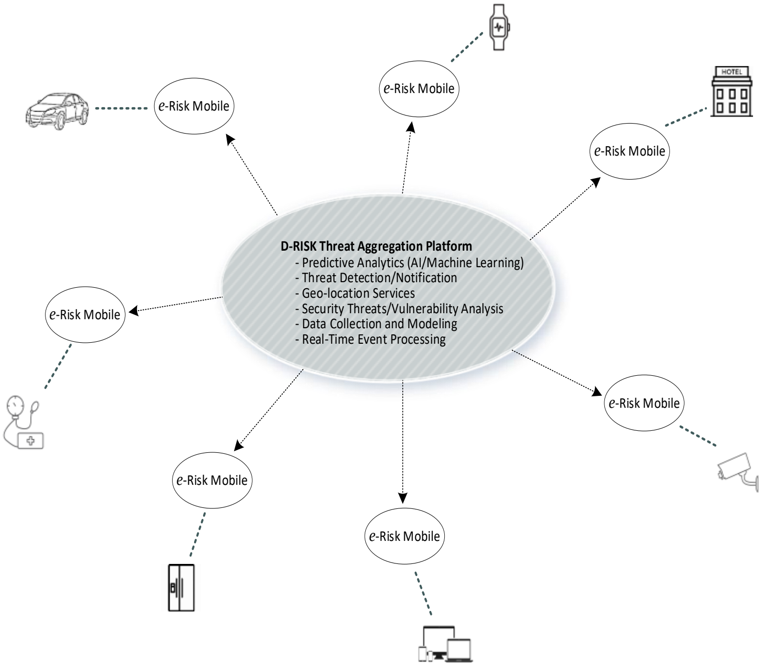
D-RISK Threat Aggregation Platform
- Predictive Analytics (AI/Machine Learning)
- Threat Detection/Notification
- Geo-location Services
- Security Threats/Vulnerability Analysis
- Data Collection and Modeling
- Real-Time Event Processing
e-Risk Mobile
e-Risk Mobile
e-Risk Mobile
e-Risk Mobile
e-Risk Mobile
e-Risk Mobile
e-Risk Mobile
e-Risk Mobile
HOTEL

***Figure 1*. D-RISK Mobile Security Architecture**

Trusted Relationships

Imagine being able to spin up a private network between two, five, twenty, or even hundreds of people instantly and communicate with each other in total privacy. Now the real question is how do you protect these communication channels from possible malicious attacks? If we think about your typical Virtual Private Network (VPN) implementation, VPNs work by creating a secure virtual tunnel through the Internet to another network or device. By encrypting your data and using private DNS servers, VPNs remain one of the most effective means of maintaining online privacy.

Nevertheless, it's important to note that anything can be hacked. This is especially true if you are a high-value target and your adversary has enough time, funds, and resources.

VPNs don’t need their encryption to be compromised to make your connection vulnerable. One of the simplest ways your data can be revealed to an outside party is via VPN leaks. Most frequently, this involves an IP leak. In the process of transmitting your data, your browser may still leak your real IP address. An attacker may not have access to your traffic data in this case, but they can trace your location.

To combat these types of issues, Cervais has developed a unique solution that enables the end-user to create what we call “Circle of Trust” (CoT), through its D-RISK Mobile Data Protector platform. Cervais CoT was designed to deliver enhanced security from scalable software attacks and common hardware attacks. This feature provides for secure Data-in-Transit and edge computing protection. It provides the end-user with unparalleled security to protect communications and data over commercial and exploited networks. Utilizing our proven authentication and encrypted framework, communication only occurs between registered, authenticated and verified D-RISK Mobile users and content being transmitted can only be understood by the intended recipients.

CIRCLE OF TRUST®

Cervais brings instant secure capabilities to endpoint devices when their own processing and memory resources are not sufficient or are not considered trusted. Cervais’ D-RISK Mobile Data Protector platform is an exceptional choice when addressing device security across a mobile generation as well as the IoT that commands high functionality to get the job done. The solution is easy to deploy and maintain, has a low cost of ownership, and can be used as a standalone solution or in conjunction with an existing enterprise device protection system.

Conclusion

Cervais is positioning itself as a major competitor to take advantage of the security issues surrounding both consumer mobile devices and the IoT market. It’s critical that Cervais understands and responds appropriately to our customers’ cybersecurity concerns. To earn consumers’ trust, we must vigorously protect customers’ data while respecting individual privacy. From connected fridges to smart door locks, interactive toys to IP connected burglar alarms, products of every type are joining the IoT. These products are simplifying daily life for consumers around the world, creating more exciting, engaging and useful products than ever before. The benefits to consumers and society are vast, and as the revolution gathers pace, connectivity in consumer products is moving from a brand differentiator, to a consumer expectation.

Headquarters Office:
20706 Pomeroy Ct.
Ashburn, VA 20147
Office: (703) 675-1619
www.cervais.com

About Cervais

Cervais® is a premier, innovative provider of world-class IT security products and systems. We deliver robust, high-performance security solutions that bring you leading-edge capability in managing risk, reducing threats, and securing technology perimeters. With IoT deployments on the rise, Cervais stands ready to help you implement comprehensive enterprise cybersecurity, identity management, planning, and security services.