# Table of Contents

Introduction  
The Game has Changed  
PCI, EMV and Looking Forward  
Developing a Security Strategy  
  Define Security Goals  
  Define Current Position  
  Define a Roadmap  
  Financial Considerations  
Conclusion  
Appendix A: Overview of Threat Types and Available Security Solutions  
  How is Data Being Accessed?  
  What Security Solutions are Available?
Introduction
In today’s ever-changing security world, Merchants need a comprehensive strategy to reduce fraud, improve security, and protect their brand’s reputation. Ever more sophisticated criminal activity is threatening their customers’ Card Holder Data (CHD), Personally Identifiable Information (PII), and merchant brands. Many merchants have taken significant strides to secure an environment with multiple challenges at its core, and while much more needs to continue to be done by other stakeholders to secure the overarching system, it is critical that merchants continue to strive to understand their own system vulnerabilities in order to protect their brand and customer data.

In response to the Merchant community’s growing concerns regarding data security threats, the Merchant Advisory Group (MAG) established a task force to evaluate current security standards, systems and tools and to create recommendations for its members. W. Capra Consulting Group in conjunction with the MAG Task Force has authored the following document to provide merchants a foundation to build a comprehensive plan to address these new threats via a security framework and an approach to delivery.

Today’s merchants face the daunting challenge of determining their exposure to growing security threats and how best to focus their security efforts to obtain a comfort level with their infrastructure, all while maintaining customer trust and brand loyalty. This white paper discusses how to create a digital privacy protection strategy based on your position on the W. Capra’s Risk Tolerance Spectrum to address these challenges. By the end of this white paper, you will understand the current threat landscape, have a basic introduction to security principles and technology, understand how to develop a comprehensive digital security strategy using the 5 Pillars Assessment approach, and how to build a framework to assess business risk versus investment.

The Game has Changed
Whether you are the CEO, CIO or Treasury Manager, the challenge of shielding your customer data from a security breach has become a top priority and enterprise wide responsibility. From the water cooler to the boardroom, daily conversations discuss the most recent incursions, the staggering numbers, and speculation about the thieves’ next target.

Recent high visibility attacks against Target, PF Chang’s, Michaels, and Sally Beauty Supply are constant reminders of the vulnerabilities that merchants must contend with. Criminal organizations are taking advantage of these system vulnerabilities, and an entire underground economy has sprung up to provide these data thieves with the tools needed to steal your company and customer information.

Security threats to merchants have changed greatly over a short period of time demonstrated by comparing a 2008 and 2012 Security Study. The 2008 study1 indicated that the most common root cause for a typical breach at that time was attributable to human error – a mistake that caused data to be exposed or vulnerable. The second most likely cause was from hacking and intrusions. Four years

---


Prepared by W. Capra Consulting Group, Inc. August 2014
later in 2012, the number one reason for most security breaches is now hacking – criminals exploiting technology vulnerabilities to break into systems and steal information. This trend is important to note as it marks the end of the era in which merchants can rely on just making sure that they have not left the proverbial front door open. Today, merchants need to make sure their systems are closed, alarmed, protected, and insured.

Another notable trend is the 25% increase in breaches due to external agents or third parties, compared to a reduction in data loss attributable to internal employees and/or business partners. This trend is proof that organized, established criminal elements have emerged as the main threat and that merchants must develop more sophisticated responses to these growing threats.

<table>
<thead>
<tr>
<th>2008 Study</th>
<th>2012 Study</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How Do Breaches Occur?</strong></td>
<td><strong>How Do Breaches Occur?</strong></td>
</tr>
<tr>
<td>62% • Attributed to a significant error</td>
<td>81% • Utilized some form of hacking</td>
</tr>
<tr>
<td>59% • Resulted from hacking and intrusions</td>
<td>59% • Incorporated malware</td>
</tr>
<tr>
<td>31% • Incorporated malicious code</td>
<td>10% • Involved physical attacks</td>
</tr>
<tr>
<td>22% • Exploited a vulnerability</td>
<td>7% • Employed social tactics</td>
</tr>
<tr>
<td>15% • Due to physical threats</td>
<td>5% • Resulted from privilege misuse</td>
</tr>
<tr>
<td><strong>Who is Behind Data Breaches?</strong></td>
<td><strong>Who is Behind Data Breaches?</strong></td>
</tr>
<tr>
<td>73% • External Agents</td>
<td>98% • External Agents</td>
</tr>
<tr>
<td>18% • Internal Employees</td>
<td>4% • Internal Employees</td>
</tr>
<tr>
<td>39% • Business Partners</td>
<td>&lt;1% • Business Partners</td>
</tr>
<tr>
<td>30% • Involved multiple parties</td>
<td>58% • Tied to activist groups</td>
</tr>
</tbody>
</table>

Source: 2012 Data Breach Investigations Report
A study conducted by the Verizon RISK team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, InfoSec and Information Security Services, Police Central-IT Crime Unit, and United States Secret Service.

Source: 2008 Data Breach Investigations Report

**PCI, EMV and Looking Forward**

Understanding the motivation behind attacks and how they are waged are the first steps in building a comprehensive plan to counter these new threats via a security framework. The following approach to Digital Security will enable a merchant to understand how current industry tools and initiatives such as PCI-DSS and EMV fit together into a comprehensive security framework. The approach will also assist merchants in defining what an acceptable risk level is for their company.
Most merchant security strategies to date have relied heavily on the PCI compliance process. PCI compliance defines the requirements that merchants must meet to protect cardholder data that is being processed, transmitted, or stored. Per the PCI Security Standards Council, PCI compliance is driven by adherence to three primary steps:

1. **Assess** – identify cardholder data, take an inventory of IT assets and business processes for payment card processing to identify vulnerabilities
2. **Remediate** – fix vulnerabilities and do not store cardholder data when you do not need it
3. **Report** – compile and submit required remediation validation records and reports

While PCI was successful at increasing awareness of security issues within merchants and creating a common standard of compliance for multiple card brands, the threats are evolving quickly and the PCI standards have had difficulty adapting to the more advanced threats that are being seen today. PCI does not specify what the merchants’ responsibilities are in the event of a breach.

As breaches have increased in frequency, more entities are positioning EMV as a potential solution for improving cardholder security. EMV will reduce specific types of fraud due to the dynamic data elements that make the card more difficult to reproduce. However, EMV by itself will not stop breaches. The main goal of EMV is to reduce the value of stolen data by making it difficult for criminals to create counterfeit cards from the stolen data. EMV may also reduce the value of stolen cards. The reduction of value in stolen cards is still to be defined as the effectiveness of Visa’s approach of Chip and Choice and other network’s CVM approach of Chip and PIN is compared. Additionally, an answer for fraudulent card-not-present transactions still needs to be defined, as EMV does not address the online world.

Furthermore, the value of EMV in preventing fraud is dependent on the number of merchants and issuers that have converted to EMV. The data from Europe and Canada indicates that EMV will significantly reduce fraud related to counterfeit cards. However, until the majority of payment transactions are EMV cards processed at EMV terminals, and a card-not-present solution is defined, the data that EMV is attempting to protect will still carry significant value in the black market and thus be a target for the organized criminal elements mentioned earlier.

Given the rate at which criminals are devising new payment fraud schemes, PCI and EMV alone are not sufficient to protect a merchant from security risks and breaches. Meeting the requirements of these industry security standards is necessary, but to protect your brand in today’s active fraud ecosystem, a more appropriate strategy is to take a holistic organizational approach toward security. This security strategy should focus on protecting the merchant brand, and should address the threats that have the highest potential to damage the company as a whole.
Developing a Security Strategy

When defining your security strategy, it is important to identify your security goals in order to determine what solutions are best fit for your organization. A strongly developed security policy developed in concert with your payments and technology strategy can help create a secure environment in which your business can thrive while, significantly reducing the risk of breach.

To assist merchants in starting the process of moving toward a more secure posture, the following steps are defined and explained in the following sections.

1. Define Security Goals
2. Review Current Position
3. Create a Roadmap to move to the Merchant’s Goal Position
4. Financial Considerations

Define Security Goals font

The key input to a merchant’s security strategy is an agreement within the organization of the merchant’s risk tolerance to a breach, or said differently what are the merchants primary security goals? On one side of the Risk Tolerance Spectrum, merchants are focused solely on maintaining compliance with industry standards such as PCI. This is the “default” security strategy that many merchants have adopted – implement only those security measures mandated by PCI and applicable government rules. Other technologies to reduce breach risk may be on a roadmap but are not a priority against other business objectives. Conversely, on the other side of the Risk Tolerance Spectrum would indicate a desire for the merchant to use best-in-class measures to protect the brand reputation. These measures include Encryption, SIEM, DLP and other security and fraud tools (details of the tools are available in Appendix 1) that will reduce the chance of a breach and minimize fraud risk. Each merchant should determine its position on the Risk Tolerance Spectrum based on its business goals and an understanding of the investment required to attain and maintain that desired end state.

Organizations should assess the likelihood that different security events will occur and make efforts to quantify the resulting impact. With this information, organizations can determine their risk tolerance and can focus their security strategy appropriately.

With an understanding of their risk tolerance, organizations can prioritize their security activities and investments against other competing objectives. It is important to understand that organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk. An organization is not wrong to focus only on compliance and not invest in best in class security as long as it understands the tradeoffs. The Risk Tolerance Spectrum diagram below provides a view on the different security stances a merchant may take.
To identify what security strategy option is most appropriate for your business, you have to understand how a breach may impact your company. To assist you in developing that understanding some challenge questions are listed below. It is possible to quantify these risks, however, as a starting point the assessment can be somewhat qualitative.

i) Value of data
   - What is the value of the data to the organization? How would it impact the organization if the cost of data were lost? Are there government regulations concerning data retention that you might be violating if the data became inaccessible? Data can have intrinsic value (i.e. PII or PCI) or it may have strategic value (expansion plans or pricing plans).

ii) Confidentiality
    - What is the risk to the organization if the data is disclosed? Financial? Legal? Regulatory?

iii) Reputation risk
    - What is the brand / reputational risk for each data type? Is there a greater risk for different types of data?

iv) Accessibility
    - How easily accessible is the data? Does the data need to be available for use 100% of the time? Is it archive data that is only rarely accessed?

v) Integrity
    - What is the impact if data is maliciously changed? Does it cost the organization money? Is it a fraud exposure?

Define Current Position
Once a merchant clearly understands its security objective, the next step is to understand how they are currently executing against those objectives. W. Capra recommends using B.A.S.E – A Security Assessment Methodology from the SANS Institute. The SANS Institute is a cooperative research and education organization that has been developing and communicating security knowledge for over two decades. The B.A.S.E methodology includes:
Baseline the existing environment
- Audit and assess the baseline environment against current and existing threats
- Secure your environment by acting on the outcomes of the assessment
- Evaluate and educate, measure the results of your security efforts and take action on additional gaps

This allows for measurement of your security approach against international definitions and standards. The methodology also aligns identified opportunities to be clearly assessed against standard definitions. The following are how opportunities are classified and the meaning of each classification.

<table>
<thead>
<tr>
<th>Quick Wins</th>
<th>Provide solid risk reduction without major procedural, architectural, or technical changes to an environment, or focus on very common attacks.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved Visibility and Attribution</td>
<td>Improve the process, architecture, and technical capabilities of organizations.</td>
</tr>
<tr>
<td>Hardened Configuration and Improved Information Security Hygiene</td>
<td>Focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Use new technologies that provide maximum security but are harder to deploy or more expensive than commoditized security solutions.</td>
</tr>
</tbody>
</table>

**Define a Roadmap**

Once you define your objectives and gaps from the current state, it is time to develop a formal security strategy and roadmap. The process of defining a roadmap depends on the large number of applications and touch points involved; more applications and touch points require more complex road mapping. There are proven methodologies that can assist in minimizing this challenge.

One such methodology is the 5 Pillars of Cyber Readiness. By incorporating the 5 Pillars of Cyber Readiness approach (listed below), to create and maintain its security strategy, a merchant can stay up to date on the latest intrusion and threats, react nimbly and quickly to those threats and protect brand integrity.

**Five Pillars of Cyber Readiness**

- **Offense informs defense** – Use knowledge of actual attacks that have compromised systems to provide the foundation to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.
- **Prioritization** – Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in your computing environment.
Metrics - Establish common metrics to provide a shared language for business executives, IT leaders, technical specialists, auditors and security officials to monitor the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

Continuous Monitoring – Carry out continuous monitoring to test and validate the effectiveness of current security measures.

Automation - Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.

Implementing the 5 Pillar methodology will require participation from different functional areas of the merchant organization and possibly require external security professionals. Merchants should expect to be faced with difficult decisions regarding the delivery of short-term business objectives versus implementing security solutions that are required for the long term.

Financial Considerations
Spending on security measures does not generate an easily quantifiable ROI. The benefit of investing in security is you reduce the direct financial risk of a data breach, along with the indirect but significant financial risk of brand damage.

In general, higher levels of security protections may require larger investments in technology and operational processes pending a merchant’s starting point. While some solutions may negate the need for other investments there has yet to be a single silver bullet that will address all security threats. Also, given the evolving nature of threats, a “defense in depth” strategy is required. A typical example to protect against data intrusion:

- Stateful firewalls to seal off the internal environment from public networks
- LAN segmentation to further isolate systems with sensitive data
- Strong Identify and Access Management (IAM) to limit access to only those individuals that need it
- Event logging to identify and record all access by authorized users to sensitive data

Prepared by W. Capra Consulting Group, Inc. August 2014
- Intrusion detection to identify attempts by unauthorized individuals to access sensitive data
- Data base encryption as a further preventive measure against theft and unauthorized access

**Conclusion**

While the MAG is focused on merchant security, it is important to note that the breach statistics highlighted within the paper represent all stakeholders and verticals. In a very complex payments ecosystem, merchants represent and are responsible for only a portion of security concerns. Breaches and data compromises can occur along a number of places within the value chain that have been highlighted by recent breaches where third party software vendors, processors and others have had major vulnerabilities.

The fact is that all merchants will continue to be the target of future attacks – even those that implement and maintain higher security levels. The focus needs to be reducing the risk of these breaches by developing, implementing, and maintaining a security strategy that works to protect both payment data as well as other personal privacy information within a merchant’s overall business strategy. An informed security strategy will put a merchant organization in a better position to avoid the significant cost of a breach as well as the accompanying negative publicity while allowing the merchant to address new business objectives such as omni-channel commerce.
Appendix A: Overview of Threat Types and Available Security Solutions

How is Data Being Accessed?

Criminals are finding your sensitive data using a variety of techniques designed to identify and exploit vulnerabilities in a merchant’s network, infrastructure and applications. Some are looking for quick hits while others invest in more sophisticated equipment and approaches. The following are four of the more common techniques.

**Phishing**

Phishing attacks target the weakest link in an organization: the innocent but careless user duped into following a link or clicking on an email attachment. Unbeknownst to the user, the attachment or link they click is laced with malware that opens a backdoor for the attacker and establishes a presence inside of a protected environment. The capability of attackers to produce fake emails mimicking the design and appearance of legitimate email has progressed to the point where it would be difficult for a trained eye to tell the difference between an official company email and a malicious one.

In the first half of 2013 alone, the Internet Policy Committee counted over 72,000 phishing attacks on 720 uniquely targeted organizations worldwide (APWG, 4). The most-targeted institution was PayPal, accounting for 18% of those attacks alone. Additionally, the top 80 targets were attacked 100 times or more during the first six months of 2013. The following chart illustrates the attack distribution by industry.

![Phishing Attacks by Industry](chart)

Source: Mandiant M-Trends® 2010: The Advanced Persistent Threat

Phishing attacks are difficult to defend – every one of your employees is a potential vulnerability. One of the most effective defenses against phishing attacks is educating users. An educated user will be less likely to open attachments and click through links that could result in an organization being breached. By coupling embedded link-inspection user awareness with a well-implemented and tuned email protection solution, organizations can significantly reduce their exposure to phishing and likelihood of compromise.
Exploit kits
Automated exploit kits employ relatively untalented attackers with powerful tools to take advantage of vulnerable targets on any network. The number of exploit kits available for purchase in the underground web fraud economy continues to grow. For example, Metasploit is one exploit kit that is very popular among the hacker community because it is free and is relatively simple to use. It offers a simple graphical user interface, giving the attacker a nice overview of payload options and targeted machines. With a few clicks of a mouse, an attacker can compromise an endpoint and begin “pivoting” across your enterprise. Pivoting is the process that begins after an attacker has established a presence inside of a targeted network. After successfully penetrating your defenses and establishing a presence within your environment, the attacker has a starting point from which they will continue to probe.

Once the adversary has compromised this initial endpoint, they will proceed to other systems by scanning each node for the presence of shared credentials or weakly stored passwords. They typically pivot until they obtain the credentials of an elevated user account, such as a shared system administrator account with full rights or a domain administrator. From here, they can access sensitive data and begin planning the exfiltration phase. Throughout this process, an experienced attacker will have made note of security barriers in place and will take steps to avoid raising any alarm with their activities.

Advanced Persistent Threats
Advanced Persistent Threats (APTs) target high-value repositories of information including systems holding trade secrets, classified information, and large numbers of payment card transactions. They are “advanced” because of their ability to evade traditional signature-based malware detection products. They are “persistent” because the code employs measures to avoid detection such as utilizing non-standard network protocols like Internet Control Message Protocol (ICMP) to communicate back to a central Command & Control (C&C) server.

APTs are difficult to detect because they are lightweight and sophisticated in their operation. The average size of an APT is only 120 kilobytes. They most often infect a system via injection into common system processes such as svchost.exe and iexplore.exe, masking their presence and making detection much more difficult. By using HTTPS for outbound connections back to their command and control server, their communications are sufficiently blended with normal encrypted sessions. They can survive reboots and in many cases reimaging by utilizing service persistence mechanisms. For these reasons, APTs are not effectively handled or detected by traditional antivirus or network security solutions.

Skimming
Skimming refers to the unauthorized interception of payment transaction data. This is typically accomplished by installation of devices that tamper with retail store equipment in order to intercept card data as it moves across the existing infrastructure. More basic card skimming involves the use of cheap and widely available hand held skimmers used by criminals who physically handle credit cards (waiters and waitresses, gas pump attendants, etc.). These compact devices feature a Magnetic Stripe Reader as well as some form of memory module that allows the criminal to quickly swipe a copy of the
magnetic strip data when out of view of the customer. More advanced skimming devices target ATMs and gas pumps and often include cameras to capture debit PINs. If the criminals can capture both the mag stripe data and the PIN, they have full access to bank accounts and can drain them over a matter of days.

What Security Solutions are Available?
There are a number of security solutions that companies have used to protect both cardholder and personal data from breaches. These solutions have typically been used in non-merchant verticals such as financial institutions and government agencies in which security requirements are even more proscriptive. The solutions below should be viewed as complimentary to existing security measures and can be layered into a merchant’s architecture to protect against multiple threats.

Data Encryption renders stolen data unusable. There are several approaches to encryption:

- **End-to-End Encryption (E2E)** - Encrypts the cardholder data from swipe all the way through to the processor, where unique decryption keys are held. A correctly implemented End-to-End encryption solution greatly reduces the effectiveness of malware or malicious devices that are monitoring the payment transaction flow – even if this malware can capture card data, the criminals will not be able to use it. The source and destination of the encrypted data have to use compatible algorithms and encryption keys, which can lock a merchant into a particular technology or supplier.

- **Point-to-Point Encryption (P2P)** – P2P is an encryption implementation in which the cardholder data is encrypted as it moves between system components (e.g. pin pad to payment switch, payment switch to processor). While similar technology is used for E2E, P2P can prove easier to implement for merchants that have multiple vendor technologies at their stores or the merchant works with multiple processors. P2P encryption also reduces the merchant dependency on a single vendor’s encryption approach. The disadvantage of P2P is that each component encrypting and decrypting data needs an encryption management approach and the data is vulnerable to skimming at any point where a component has decrypted it. The P2P encryption method requires merchants to either internally host the security module for encryption/decryption or can elect to outsource this service to a 3rd party provider. Regardless of the architecture chosen, a merchant is still responsible for the data when present in their environment.

- **Tokenization** - The replacement of cardholder data with a unique “token” or identifier that cannot be turned back into the card number. Card data is still transmitted from the card swipe unit to the processor in the initial authorization request, but the processor returns a Token in the response. From that point forward, the payment related data flows do not contain any useable card data-only the token issuer can translate the token back into a card number. There are two approaches to tokenization:
• **Static Tokenization** - assignment of one token per unique card number for that particular merchant. This keeps tokenization costs lower, but is less secure than Dynamic Tokenization

• **Dynamic Tokenization** - assignment of a unique token to every transaction. Provides higher security but puts more demands on the components of your payments architecture

A merchants’ processor can provide the tokenization solution or merchants can elect to use a 3rd party solution. Most implementations of tokenization and associated card vaults are implemented outside of the merchant environment to reduce the amount of cardholder data within the environment. There is a tremendous amount of discussion regarding tokenization for mobile payments. The mobile token concept is:

- A mobile payment user would enter their card data once
- The mobile payment host would store the card data in a secure vault and return a token to the mobile device
- All subsequent mobile payments by that individual would send the token rather than an actual card number
- Lower interchange qualification may be available in the future if the network has defined a relationship with the processors token scheme

Due to the higher security provided by this approach, card networks are considering using tokens as a key criteria when looking at new interchange categories for mobile-based transactions.

• **Hashing**: A one-way formula used to generate a replacement value for each card number. These values can typically be used for analytics work where the merchant needs to identify the customer across multiple transactions, but does not need the actual card number. Hashing is normally used for the payments flow, because it cannot be turned back into an actual number.

• **Encrypting Data at Rest**: The technologies above are most often applied to card data as it passes through your system components during the transaction life cycle. Encryption can also be used to encrypt transaction data while at rest, typically in site systems that maintain transaction logs, card settlement and dispute resolution systems. Encrypting card data at rest is a PCI requirement; encrypting all of the transaction information reduces the probability that a hacker who gains access to your environment can extract useable data.

When assessing which of the following strategies to use there are a number of merchant considerations:
1. The merchant must understand how the account number is used throughout the full payment lifecycle—authorization, routing, settlement, refunds/returns, exception item processing, fraud management and data analytics.

2. The merchant must understand how the cardholder data is used in current environment—the encryption and tokenization/hashing solutions must be compatible with existing data field requirements (e.g. number of characters, numeric versus alpha-numeric characters, etc.)

3. Some technologies increase dependency on your card processor. Use of a third party solution can mitigate this dependency but can complicate the card processing flows.

4. Maintaining consistent tokens for card present and card-not-present channels

5. Ability to convert existing cardholder data to a tokenized value or to obtain the original card number when changing token vendors

**Digital Security Policy Enforcement**

In addition to securing payment data flows, merchants can implement security measures to prevent unauthorized access or theft of a wide variety of data types.

**Data Loss Prevention (DLP)** - Systems designed to prevent breach of data by monitoring data at rest, data in motion and data in use. DLP tools use industry and merchant specific rules to help an organization govern the location, flow, and usage of sensitive data such as card data, personal information and intellectual property.

- **Examples of DLP Protected Data:**
  - An internal spreadsheet containing cardholder data, including full card numbers is accidentally attached to an email. Through a DLP rule flagging 16 digit numbers with a corresponding date in mm/yy format, the DLP software will not allow the email system to send this spreadsheet.
  - A contract programmer working on the HR System attempts to download personal data including social security numbers and birthdates to a USB drive. The DLP rules will block this attempt.

**Security Information and Event Management (SIEM)**- Systems that allows an organization to monitor and act on activity throughout the entire IT spectrum to provide a consolidated view of security activity based on designed system flags and event correlation. Alerts are triggered based on automated analysis of activity, which can then trigger system action, based on If This, Then That defined rules.

- **Example of SIEM in use:**
  - SIEM policy in place for identifying failed login events to a server where customer data is stored, along with a rule that disables that ID after a number of attempts, and alerts the system administrator.
- SEIM policy that generates an alert surrounding executable files not whitelisted to execute on that particular server.

**Application Control** - The ability to define, via whitelisting, the executables that are allowed to run on a platform, along with inputs and outputs that can interact directly with an application. In direct contrast to the operation of virus scanning software, application control allows a quick check of the whitelisted, allowable functions to ensure no malicious software is running on the platform.

  - **Application Control in use**: Many types of malware attempt to pass themselves off as popular applications. Without clearly defined rules for application use and deployment, this malware can easily impact company applications. Through application control policies, only whitelisted applications that meet specific criteria (e.g. file size, check sum) can be used or deployed.
  - Currently Application control is a common security strategy for companies that have to extend the life of their Windows XP deployments

What becomes apparent when assessing the different security technologies is that each provides different types of protection. The following chart helps to depict how different security technologies protect different entities.