White Paper
Intel Information Technology
Computer Manufacturing
Enterprise Security

Defense in Depth Strategy Optimizes Security

Intel IT developed a defense in depth strategy that optimizes security using interlocking prediction, prevention, detection, and response capabilities. We recognize that attackers are human opponents who constantly evolve new tactics and that it would be prohibitively expensive—and near impossible—to protect against every vulnerability. Our strategy uses prediction to gain insights into the most likely threats, attack methods, and targets. This allows us to proactively and efficiently focus our prevention, detection, and response resources. Learnings from each of these areas feeds back to our prediction teams, creating a performance improvement loop that helps our strategy continually evolve to intercept emerging threats.

Matthew Rosenquist, Intel Corporation

September 2008

IT@Intel

Executive Summary

Intel IT developed a defense in depth strategy that optimizes security using interlocking prediction, prevention, detection, and response capabilities.

The strategy is based on the fact that attackers are living opponents who constantly evolve new tactics as we create new defenses. It would be prohibitively expensive, and probably impossible, to protect against every vulnerability. Our strategy uses prediction to efficiently and proactively focus prevention, detection, and response resources on the most likely attackers and methods.

- **Prediction.** Prediction capabilities include analyzing emerging threats as well as classifying likely threat agents and their methods.
- **Prevention.** Prevention includes education to create a threat-aware workforce as well as technology barriers.
- **Detection.** Security incidents and intruders must be promptly identified, contained, and eradicated to minimize losses.
- **Response.** Our IT emergency response process (ITERP) has the authority to harness the resources of the entire organization to quickly contain and recover from attacks.

Each of these four capabilities—prediction, prevention, detection, and response—feeds information into the other capabilities. For example, during response to attacks, ITERP acquires information about attackers and methods that we use to improve our prediction capability. This creates a performance improvement loop that helps our strategy continually evolve to intercept the next emerging threat.

Our strategy uses prediction to focus prevention, detection, and response resources on the most likely attackers and methods.

Contents

Business Challenge

Managing an organization's information security efforts can be frustrating for IT departments. Consider that many IT technical problems are single-faceted: A network line goes down; a power supply burns out. We identify the problem, fix it, and document it so we can quickly apply the same solution the next time the event occurs. It is logical, methodical, and even predictable.

Security threats are not so easy to deal with. They are unfamiliar territory, foreign in nature, evasive, and dynamic. This fundamental difference causes frustration and can lead to inefficient resource models and a weak security posture. Without a good strategy, an organization may waste resources and its defenses may become ineffective.

The difference is in the nature of the threat. A failed power supply is a straightforward obstacle. Swap out the device and you return to a normal state. In contrast, information security threats are people—people who are intelligent, creative, persistent, and adaptive. These multi-faceted threats can wreak havoc on an immature security organization. There is a big difference between a technical obstacle and a dynamic opposing force. Attackers constantly develop new methods of attack; they respond to what we do and adjust their tactics to achieve their goals. Security is an adversarial competition, more like playing a chess game than fixing a spark plug.

The bad guys are smart, fast, agile, share knowledge with their peers, and, in most cases, maintain the attack initiative. The difference in mentality between these two opposing forces gives attackers a key advantage. Security specialists often believe they must protect every asset from every type of attack, and therefore must close every vulnerability. This leads to frantic work and frustration about lack of resources, and the resulting effort may be seen by the company as a significant unnecessary overhead. Attackers have a different perspective. In order to win, they need only to succeed once. Find one hole, one weakness, and the trophy is theirs. An endless sea of ripe targets lies before them. If they don't like what they see, they can adapt, move on, and target something else; time is on their side.

The attackers themselves have evolved over time. Early viruses were created by novices: They were often badly coded and easily detected once identified. Now, there is a much larger spectrum of threats. Rather than aiming to cause disruption, these attackers may wish to remain invisible; they may be stealthy, quietly grabbing information or doing far worse. Attackers may be professionals performing theft, espionage, blackmail, or other nefarious activities which can impact daily operations. They may be well funded, experts in their fields, and some may be supported by competing companies, organized crime, or governments. Some of the biggest threats are internal: the trusted vendors, employees, and contractors to whom we have granted access and who covet what they can see.

The scope and complexity of these threats calls for a comprehensive approach to security. Because attackers constantly evolve new attack methods, simply fixing a problem in isolation will not help predict and prevent new ones. As a simple example, if we detect an e-mail virus and respond by cleaning infected systems and blocking that message throughout the enterprise, the attacker may simply create a new version and proliferate it—and do so much faster than we can clean it up.

We recognize that there are an almost infinite number of vulnerabilities, and we cannot protect against everyone and everything. Even if possible, it would be prohibitively expensive. Attackers can leverage vulnerabilities in people, computing systems, and communication networks. This represents a massive potential target landscape to protect from edge to edge. No single solution provides this comprehensive security.

We therefore need to optimize our security strategy, focusing our resources to protect and reduce impact to the organization in the most efficient way. This means we need complementary capabilities that enable us to predict the most likely target areas, prevent the most likely attack methods, quickly detect penetrations, and respond effectively to limit damage and restore a normal state of operations.

The concept of this defense in depth strategy is straightforward: establish a system of capabilities and services aligned to attackers, their objectives, and the methods they are most likely to attempt. Couple this with an understanding that attackers will succeed sometimes, and that at every turn there exists a learning opportunity we can use to improve the system. Because information security is such a dynamic area, our strategy has to be flexible enough to adapt as new threats emerge.

Solution

Over the past six years, Intel IT has evolved a defense in depth strategy to meet these challenges. Our strategy has been proven to work over time in many different security disciplines. We have found that this strategy is highly effective at providing overall security assurance, as well as establishing cost-effective, scalable, and adaptive programs that keep pace with changing threats.

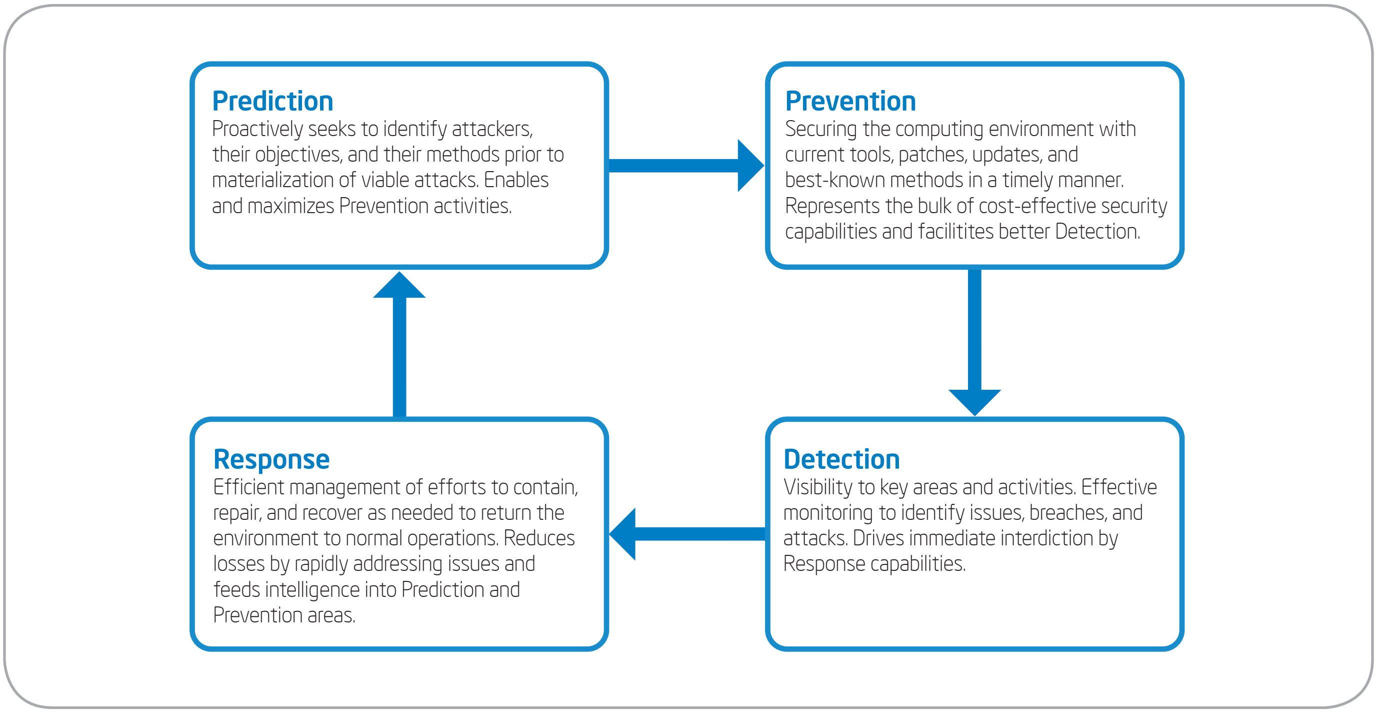
Our strategy evolved as we established our IT information risk and security organization, building on information warfare theory and venerable security approaches. We took the mature IT security model of prevention, detection, and response, and added a fourth key element: prediction.

The addition of prediction creates the continually evolving structure that is necessary to adapt to the fluid nature of information security threats. Prediction gives us insights into the most likely threats, methods, and targets, which allow us to efficiently focus resources in the prevention, detection, and response areas. Conversely, learnings in these areas feed back into the prediction teams to promote better assessments, forming a continual performance improvement loop as shown in Figure 1.

Our strategy enables us to reduce the risk of losses as well as the associated cost. The earlier we can interdict a threat, the more we reduce the potential loss. The cost of predicting or preventing an attack is a fraction of the cost of responding to a successful attack, as shown in Figure 2.

Prediction

Prediction is an invaluable first step in the efficient use of security resources. Although the truly paranoid may disagree, not everyone



Prediction
Proactively seeks to identify attackers, their objectives, and their methods prior to materialization of viable attacks. Enables and maximizes Prevention activities.

Prevention
Securing the computing environment with current tools, patches, updates, and best-known methods in a timely manner. Represents the bulk of cost-effective security capabilities and facilitites better Detection.

Detection
Visibility to key areas and activities. Effective monitoring to identify issues, breaches, and attacks. Drives immediate interdiction by Response capabilities.

Response
Efficient management of efforts to contain, repair, and recover as needed to return the environment to normal operations. Reduces losses by rapidly addressing issues and feeds intelligence into Prediction and Prevention areas.

Figure 1. Intel IT's defense in depth strategy provides a performance improvement loop that helps improve our security strategy.

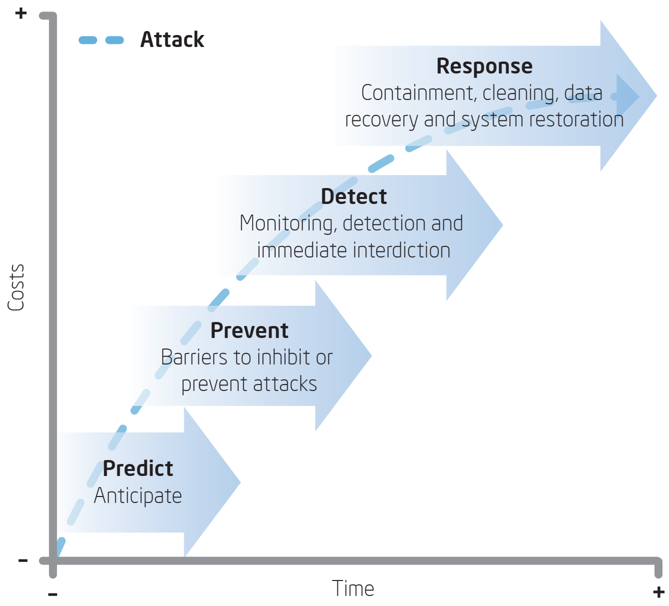

+
Attack
Response
Containment, cleaning, data recovery and system restoration
Detect
Monitoring, detection and immediate interdiction
Prevent
Barriers to inhibit or prevent attacks
Predict
Anticipate
Costs
-
-
Time
+

Figure 2. Early interception of attacks reduces costs.

is interested in attacking an organization. Furthermore, within the enormous realm of possible attack methods and vulnerabilities, it is more than likely only a few would ever be employed.

Security professionals understand the relationship between attacks and the environment they protect. They marshal their resources to intercept the most likely attack vectors for the greatest effect. Knowing where to focus becomes a significant tactical advantage.

This process involves understanding why the organization would be attacked, the potential attackers and methods, and the most probable targets. Typically, attackers are most likely to choose the path of least resistance. Once we understand their viewpoint, we can focus our prevention and detection resources on the most likely threats and targets, efficiently deploying our resources to deliver the maximum protection.

This approach has many benefits. Just because a vulnerability is a plausible target does not mean it is a probable one. Why spend energy on vulnerabilities that will never be exploited? We can manage risk by deciding where to allocate spending and effort, instead of blindly throwing money at security and hoping for the best. Prediction enables us to be proactive. This fundamentally changes the game. Traditionally, attackers have maintained the initiative, utilizing the latest technology and techniques well before target organizations do so. Defenders are in a constant state of trying to catch up as they respond to attacks. The cycle continues as attackers apply a stream of new attacks and defenders struggle to reorganize and adjust.

Ironically, successful attacks become security departments' justification for requesting funds to strengthen defenses. Without new attacks and the resulting pain and loss, there is little motivation for security spending. Unchecked, this cycle can drain excessive money from the enterprise.

Being proactive turns the tide in favor of security. If we can predict new attacks with confidence, management can invoke countermeasures before losses occur. It becomes an entirely different situation where security maintains the initiative and therefore counters the attackers' advantage.

The prediction approach also helps us avoid the common pitfalls associated with focusing exclusively on vulnerability assessments. The industry is discovering a rapidly growing number of vulnerabilities in hardware, software, and users. Many of these are obscure, complex, and do not apply to environments with good security practices. However, security groups may feel compelled to close all vulnerabilities—an ever-increasing challenge that requires more and more resources over time, and has side effects such as increased downtime and deployment errors.

Although vulnerability assessments are valuable, they are misleading if used as the only information source for prediction. Understanding your opponent is fundamentally different and equally as important as knowing the weaknesses in your environment. The result of relying exclusively on vulnerability assessments will be expending effort on areas that will never be targeted. Consequently, fewer resources will be available for the areas that are actually under siege.

Over the past few years, Intel has developed a number of prediction capabilities. These are teams that include experts drawn from multiple areas within the company.

- Emerging threats team. This broad cross-functional team of professionals continuously discusses emerging trends and events. We scour the latest news, research, and conversations from the security and attacker communities. These discussions feed into risk assessments and provide input for our threat horizon team and threat agent group.
- Threat horizon team. This narrower cross-functional team discusses expected future trends and publishes a semi-annual internal report for Intel. We describe threats, expected future trends, and complementary recommendations for specific actions.
- Threat agent team. This team works to classify different attackers, or threat agents, in order to understand who is likely to attack, their methods, as well as their motivations. We are establishing a framework to better understand and predict the underlying sources of threats. This information is shared internally and, more recently, with external partners, including a government security agency.
- Rapid risk assessment team. These technical experts meet often to track the enormous number of emerging vulnerabilities and determine the risk to our environment. They document the risk, escalate critical issues, and provide mitigation recommendations.
- Security Center of Excellence (SeCOE). This team evaluates Intel products for security and privacy before we use them internally or release them to our customers. After release, they continue to watch for weaknesses and quickly address them. IT security and SeCOE teams work closely together in threat prediction.

Through the efforts of these groups, Intel is able to look ahead and plan how best to outmaneuver imminent threats. We use the intelligence that these teams gather in our prevention and detection efforts.

Prevention

Every organization wants to deter and prevent attacks because doing so delivers a better return on investment (ROI) than responding to attacks that have already occurred. Avoiding loss is a measure of security effectiveness and efficiency.

Using insights gained from prediction efforts, we can efficiently create a frontline of defense that eliminates the easy attacks and protects critical assets against more-determined attackers.

Achieving the maximum benefit requires a combination of technical and behavioral controls. Unfortunately, many organizations focus primarily on technical barriers and do not pay enough attention to behavioral aspects such as creating a security-aware workforce. In reality, effective information security relies as much on behavior as on technical controls. The Intel security community realizes that security involves dealing with people—not just attackers but also victims and defenders. An organization may have the best prevention technology available, but without security-aware employees it will still suffer unnecessarily because human intervention can bypass most technical controls. Even the best firewall is worthless if an employee clicks on a malicious e-mail attachment that downloads a virus to his system.

Technical solutions are still essential, of course, because an organization may have well-trained employees but there will still be threats, including unforeseen events, that only technology can intercept. For example, spam would quickly drown our inboxes if we did not use automated filters. Solutions include anti-malware, system hardening, network and data compartmentalization, authorization and authentication controls; host and network firewalls; and timely automated patching to name a few. From the network perspective, the main battle line is the corporate demilitarized zone (DMZ) where the Internet connects to the internal network. Security organizations prevent communications attacks mostly with inline high-speed automated technical solutions such as firewalls, proxies, and other DMZ controls, as well as secure device configurations and a good network architecture plan. These must be maintained and continually optimized for emerging and anticipated threats in order to remain highly effective.

At Intel, we have complemented prevention technologies with a major internal education effort. With backing from senior management, we established security policies that define good security practices that all employees should follow. We made education in these policies mandatory for all employees. The policies include such simple rules as using strong passwords, handling sensitive data appropriately, and not opening e-mail attachments from untrusted sources.

Our combination of technical and behavioral controls results in a strong and flexible defense posture against most threats.

Detection

It is impossible to establish and maintain absolute security. Unfortunately, a number of attacks will eventually slip past defenses. To minimize losses, security incidents must be promptly identified and contained, and intruders removed as a future threat.

The first step is successful detection. This is not easy because of the trend toward stealthier assaults. Threat agents want to compromise systems without raising attention, to increase the length of time that they can continue their attacks.

Detection and monitoring capabilities identify the incursions, violations of policy, and even attempts to escape. The key functions are to ascertain when the prevention defenses have been breached and track the actions of intruders. These capabilities sound the alarm and enable responders to rapidly trace the source and comprehend the scope of the problem.

When it comes to detection, speed and accuracy are most important. Attacks could originate from anywhere. Detection capabilities are the eyes of security, but it is impossible to watch every corner of the computing landscape because the cost would be prohibitive. Therefore, it is vital that detection capabilities focus on the right areas and events. Our prediction capabilities help us assess the most likely attacks and determine what to watch as well as how best to monitor it.

In some cases, detection capabilities can substitute for costly or unavailable prevention measures. If a patch to a known vulnerability is not ready for deployment, detection systems can watch for attacks until a permanent solution is ready. For the large number of obscure attacks, detection might be the best long-term solution. It may not make sense to invest in expensive security solutions for highly unlikely attacks; however, ignoring them is not practical either. Monitoring can be the optimal solution to provide peace of mind at low cost. If such attacks are ever detected, the company can then invoke a rapid response and invest in prevention measures with confidence.

Not all detection is technology based. We may be alerted by an employee or business partner who notices something suspicious. This is another example that shows how security-aware users are a valued resource. Our employees are trained on how to report issues. Reporting is worthless if the correct people are not notified in a timely manner, so the organization is set up to alert the right security teams quickly for severe issues. Employees report spam, virus infections, unusual system activity, and theft, as well as concerns when sensitive data is exposed to persons who don't have a business need. With proper care and support, social reinforcement promotes more secure behavior; people begin to act and work more securely over time.

Detection directly feeds into the response processes and tools, and also contributes to our prediction and prevention areas. If we find that attackers have used an unexpected path, we can adjust our prediction and prevention capabilities accordingly. This feedback loop continually strengthens Intel's overall security posture and initiates adaptations necessary to remain secure.

Response

When an attack succeeds, swift and effective response is vital. It is the response team's job to reverse the downward spiral and restore normal operations. Time is on the side of the attacker, and every lost hour can result in a dramatic increase in the impact, confusion, and cost. An inability to restore the organization to a safe and normal state translates to lost money, time, resources, and productivity. If the loss becomes too large, an organization may simply be unable to recover. Such catastrophic scenarios are executives' nightmares.

Containing the security event is critical. This requires having the right processes, people, tools, and capabilities already in place. The work required to restore normal operations can range from minor effort to catastrophic recovery. The earlier the detection capabilities alert the organization, the easier it is to recover. Stealthy attackers who have had plenty of time to burrow deep into the environment and achieve their objectives pose a greater problem. The longer they operate unchecked, the more damage they can cause, and the situation becomes progressively more difficult to resolve.

Intel currently maintains a very effective response capability. Years ago, we discovered Intel was less prepared to respond to cyber crises than to other types of disasters. As a result, we created and improved a number of different processes, including the inception of the IT emergency response process (ITERP). ITERP has become a success story for Intel, allowing Intel to rapidly and effectively respond to crises.

We based the ITERP structure on proven emergency-response organizations, with a hierarchical control structure headed by a single empowered incident commander. ITERP includes a dedicated, top-level team as well as professionals from throughout the company. During a crisis, this pool of experts forms the working teams that evaluate the problem and execute the functional plans to recovery. Intelligence, server, network, client, enterprise application, and selected business groups form the backbone of the team. Employees undergo mandatory ITERP training so that an awareness of ITERP's authority permeates the company. As a result of this structure and training, as well as rapid communication in times of crisis, ITERP can draw on the resources of the enterprise to respond quickly when needed.

During a crisis, the incident commander has broad and recognized authority, and is the focal point for solving the problem. The commander is empowered in many cases to take action without the bureaucracy constraints of having to request resources or approval from senior management. This facilitates rapid and flexible action to contain the problem. Authority flows down through the ITERP structure. Employees know they must follow the directions of ITERP teams and comply with requests immediately.

This enables Intel to marshal massive resources on short notice. We focus these resources to eliminate a small problem quickly, before it becomes a larger issue.

This structure has proven so effective that we now apply the ITERP process in a proactive way to situations that have not yet occurred but that we believe to be imminent. The predictive teams trigger this response as part of their analysis of upcoming issues. For example, if they discover a new vulnerability that is likely to severely impact the company, ITERP is activated and we apply our resources to mitigate the risk through filters, patching, upgrades, and end user communication.

We use information gathered by ITERP to complete the defense in depth cycle by improving our prediction capabilities. Response to events provides a valuable learning opportunity. When we respond to an attack, we acquire information that identifies likely attackers, their methods, and a more accurate estimate of potential damage. This information is particularly valuable because threats to Intel may differ significantly from those affecting other companies. This highly specific information complements the general information about current threats that we receive from external industry sources. We feed our learnings back to the prediction teams. This enables them to refine their prediction assessments, leading to more effective prevention, detection, and, ultimately, response.

Results

Proliferation of our defense in depth methodology has resulted in more efficient business decisions. It simplifies threat assessment, opens options to creatively manage risk, and enables us to avoid frenetically trying to fix every vulnerability. Instead, the security organization can balance security with business objectives by choosing which issues we should act to prevent and which we should monitor and prepare for. This has saved Intel considerable time and resources.

Defense in depth is a structure designed to promote continual improvement. With prediction and detection feeding information to response teams, Intel has continually improved ITERP over the years. As a result, we have reduced the time it takes to contain events. In 2007, we experienced a record high number of cyber events, with a total of 118 compared to 74 in 2006. The time needed to contain cyber events averaged 2.43 days, down from 5 days in 2006. By quickly containing cyber events and mitigating their impacts, we prevented significant impact to Intel despite the increased number of events.

The strategy also provides an efficient way to evaluate proposals for new security technologies and projects. A quick assessment can reveal how well a potential project fits into our existing prediction-prevention-detection-response framework before we embark on a detailed, resource-intensive analysis. It can also help us determine whether a project is redundant or fills a gap.

We used the strategy effectively when implementing Terminus, an internally developed client tool, in 2003. Terminus resided on each IT-issued desktop and notebook PC. Each time a system connected to Intel's global production network, Terminus verified that its OS and application patches were current. It checked that security tools were up to date and operating correctly, and looked for traces of specific malware. If anything was amiss, it denied access and redirected the connection to a secure network where the system could be cleaned if necessary and brought back into compliance.

Refusing network access to unsecured systems was a huge success. Previously, we either had to manually clean systems or allow them to connect to the network in order to be cleaned. While connected, an infected system could try to spread its malware. Terminus changed the game. It protected the network while notifying end users of problems and empowering them to resolve the issues.

When we evaluated the proposal for Terminus, mapping its capabilities to the defense in depth structure illuminated its potential value. Its primary role was to establish confidence in systems connecting to the network, a preventative control through detection routines. However, it became apparent that Terminus could do much more.

During a crisis, Terminus was quickly able to determine which systems were infected, which were vulnerable, and even push fixes down the wire—all at the critical point when systems attach to the network. Crisis response teams could receive near real-time reports about the number of systems compromised and patched. Prediction teams could correlate where malware was originating and plot an expected future path. Delivery mechanisms embedded within the tool could make changes to systems as needed. Terminus was tactically employed by all defense in depth groups to collectively achieve strategic security goals.

Once Terminus was in place, we were able to retire other programs that provided duplicate services, providing cost savings and enabling us to focus our resources.

As a multi-capability tool, Terminus filled gaps and helped integrate our prevention, detection, and response teams. Terminus was recently retired, but had a long and valuable life within Intel. When it came time to replace the tool, understanding its role helped us define the characteristics of its replacement and provided continuity of critical security services.

Conclusion

Defense in depth provides a comprehensive structure for managing information security. It helps ensure that we understand and address fundamental aspects of security, yet does not impede the flexibility needed to manage risk. Applied consistently, it aligns programs, resources, and initiatives to the goal of achieving optimal security.

At Intel, we incorporate the concepts of defense in depth into our strategies, architecture, project work, and daily operations to drive security decisions. We understand we cannot control all aspects of security, nor should we try. Instead, we invest in overlapping, complementary controls to provide an efficient defense.

Our strategy has proved its effectiveness for nearly six years. It has allowed us to be as agile as much smaller organizations. Our prediction capabilities enable us to be proactive in identifying the most likely threats and creating prevention capabilities, minimizing the possibility that attacks will succeed. With ITERP, we respond quickly to contain attacks. By feeding information from response and detection back to our prediction and prevention areas, we reduce the chance of future incursions.

By remaining effective over time, the defense in depth strategy has also demonstrated that it is flexible enough to adapt to new threats as they emerge. We hope that publishing the strategy will encourage other organizations to take advantage of this approach.

www.intel.com/IT

Author

Matthew Rosenquist is an information security strategist with Intel Information Technology.

Acronyms

DMZ	demilitarized zone	ROI	return on investment
ITERP	IT emergency response process	SeCOE	Security Center of Excellence

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Printed in USA
0908/IPKA/KC/PDF

♻ Please Recycle
320076-001US