



Building Resilience in a Digital Enterprise

Transforming from compliance to risk management

Risk Management Builds Resilience

To be successful in business today, an enterprise must operate securely in the cyberdomain. We're in a period of unprecedented change where transformation and disruptive technologies are the new constant. This transformation and disruption are having a profound effect on security perception and architecture within the business. Security is recognized as an essential element to managing the risk caused by disruption. More importantly, organizations realize that resilience is necessary to take advantage of the innovation made possible by transformative technology. Operating reliable digital services and safeguarding sensitive data are essential to establishing trust with customers and maintaining business continuity. Many organizations today have established a good foundation of cyberdefense within their enterprise. That foundation was primarily compliance-driven and built on best practice or industry regulation. As the risk from targeted threats continues to grow, organizations are seeking more value from their security investments and looking to embed cybersecurity decisions into the normal risk management process of the business. Organizations are looking to embed security into the culture and enterprise architecture of the business to ensure its resilience for the long term and reap the benefits of the current revolution. Building a strategy for resilience by growing capability towards a trusted level will help ensure sustained business continuity in the face of any threat.

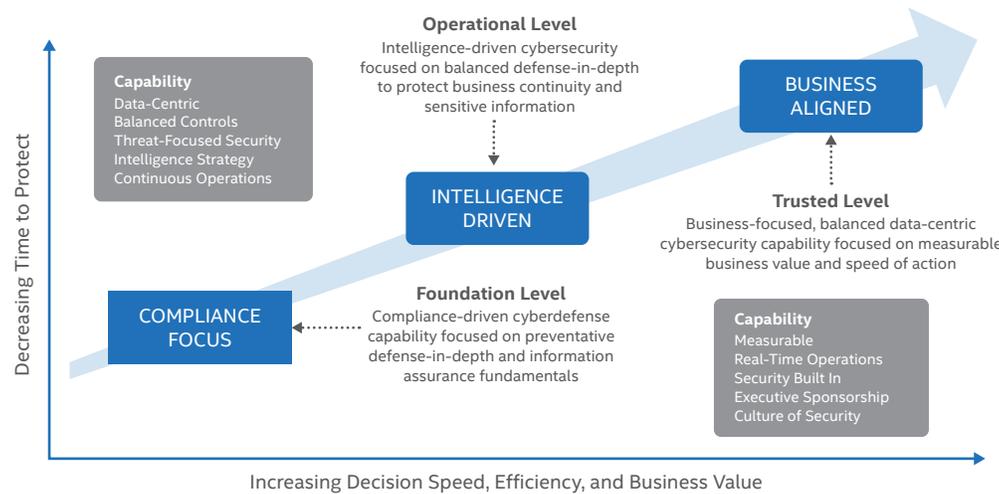


Figure 1. Strategic steps to build a cyber resilient business environment.

Solution Brief

This capability roadmap defines the journey an organization can take to operationalize security and move towards a resilient business environment. A digital enterprise faces a number of challenges to move along this journey. The first challenge is *attack speed and sophistication*. A typical targeted attack may have taken months of planning but typically only takes a few hours to complete. This presents a serious challenge to defenders who have to prevent and respond at the speed of the network.

Unfortunately, breaches usually aren't discovered for weeks, as lack of continuous monitoring, compounded by an incomplete sensor grid and insufficient threat intelligence, slows speed of response. Enterprise security operations are faced with analysing millions of security events and suspicious files to find targeted threats. Often this analysis is manual or short-term, which greatly reduces the scope and speed of the response process. It is increasingly important to fully integrate sensor technology with automated malware analysis capability and intelligence to produce high-fidelity indicators. The more accurate the initial indicator, the faster security operations can respond to an attack. The second challenge is *prioritization*. With so many different operating environments and budgets tight, where does an organization prioritize their security investments? A key tenet of operational level security is "Offense informs defense." In other words, prioritize security investments to protect sensitive data from targeted threat actors. Several models exist that define these methods, and they can be used to maximize the effectiveness of balanced security control investments. The following sections describe those models, as well as several critical building blocks, to help a digital enterprise grow their cybersecurity maturity to an *operational* level and become more cyber resilient.

Data-Centric Business

For business, it is all about the data. Enterprises cannot move fast enough to create new value from Big Data and analytics. However, in security, we are still too device-centric in terms of protection. To manage the risk against targeted attacks, an organization must shift focus from protecting devices and networks to protecting data. That is the only way a digital enterprise can both enable the business and be more effective at managing this risk. There are two general processes to data-centricity in security. First, identify high-value data assets, and second, put a ring fence around them. Identifying sensitive data can be difficult. However, almost all enterprises can be broken down simply into three data operating environments: traditional, operational, and supplier.

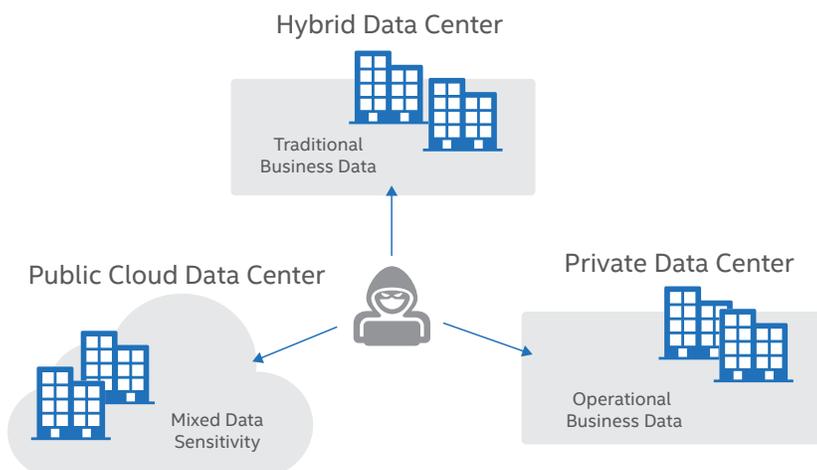


Figure 2. Today's data centers.

Solution Brief

The “traditional” environment is typically the office environment, with applications like ERP and finance holding the most valuable data. The “operational” environment typically represents mission-critical systems and houses critical intellectual property. The “supplier” environment can be external cloud providers or other business partners. The interconnectivity between the different operating environments creates security dependencies that increase the risk of data loss. This process establishes a baseline of data awareness and supports increasing levels of control based on system criticality. Secondly, an organization must break down the information silos and learn to use data more effectively to identify a risk from an external or internal attacker much faster. With this foundation in place, an organization can monitor behaviour patterns and potential violations that could signal a need for intervention or incident response.

Balanced Controls

For many years, most enterprises focused on prevention as the only means of cybersecurity. Organizations deployed a varied set of security technologies and operated them independently. However, targeted, persistent threats, whether insider or external, are multifaceted problems—a one-dimensional approach to security increases the risk to the business. To be resilient, an enterprise must adopt a balanced, continuous approach to cybersecurity and grow their capability to *anticipate, identify, prevent, detect, respond, and recover* from incidents in the cyberdomain.

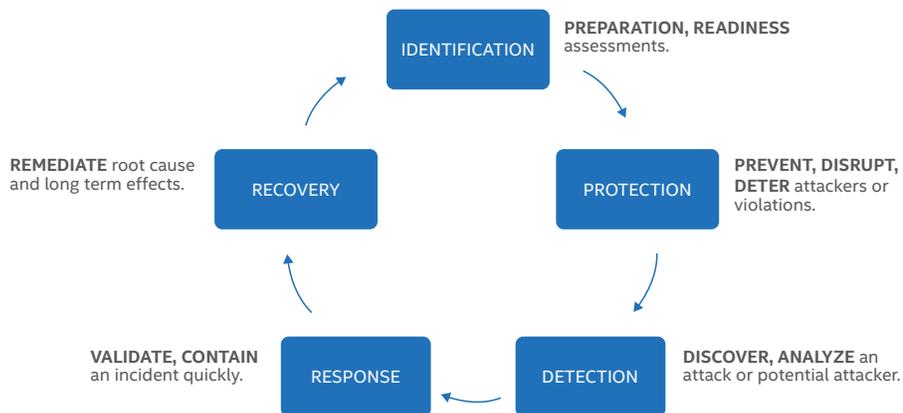


Figure 3. A balanced approach to enterprise security increases resilience.

The NIST cybersecurity framework describes the key capabilities needed to balance security. The framework is a compilation of risk-based guidelines to help an organization assess current capability and prioritize future investment to meet goals. In addition to the NIST framework, the SANS Top 20 Critical Security Controls provide a highly focused set of cyberdefense actions based on collective community input that will help mitigate many common and targeted threats. The combination of NIST Cyber Security Framework with SANS Critical Security Controls provides an excellent roadmap of impactful security actions.

Threat-Focused

According to the SANS Critical Security Controls, one of the key tenets of an effective a cyberdefense program is “Offense Informs Defense.” The adversary attack chain is an example of how offense can inform cyberdefense. These models closely replicate the tactics, techniques, and procedures used by an attacker to steal sensitive data, plant destructive malware, or gain a foothold for later actions. By understanding the adversaries’ methods, an enterprise can prioritize cyberdefense investments to those that have the most impact on risk reduction.

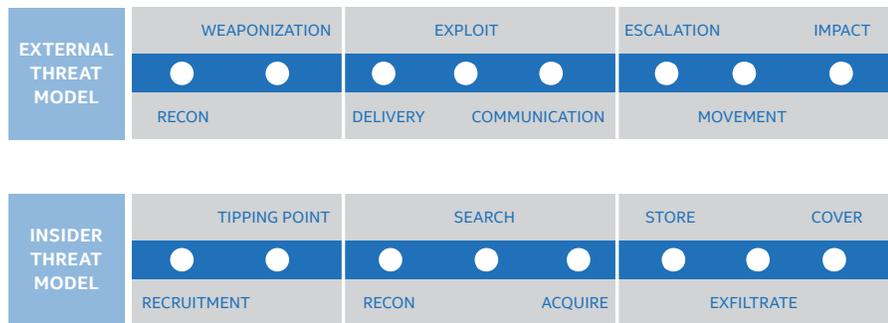


Figure 4. External and insider threat models.

The earlier an attack is prevented or detected, the less risk to the business. However, as an attacker moves through the chain, it becomes increasingly more difficult to prevent or detect the activity. An enterprise can reduce the risk of a targeted external threat having an impact by focusing anti-malware preventive and detection controls against the middle stages of the attack chain. Additionally, an enterprise can leverage the attack chains to measure real security capability. Each step represents an area where a control can be employed to reduce risk. As stated above, an organization can use various cybersecurity control frameworks, such as those developed by NIST or SANS, to match requirements against each stage in the attack chain. The following chart loosely maps the two frameworks to the stages of the external threat attack chain.

NIST	SANS CSC	Attack Chain Stages
Prepare	SANS CSC 1, 2, 3, 4, 9, 10, 17, 19, 20	All Stages
Prevent	SANS CSC 5, 7, 11, 12, 13, 15	Delivery, Exploit
Detect	SANS CSC 5, 14, 16, 18, 20	Exploit, Communication, Movement
Respond	SANS CSC 8, 18, 20	Exploit, Communication, Movement
Recover		Impact

Table 1. NIST and SANS frameworks mapped against attack chain stages.

By mapping to the attack chain, an organization can identify its security gaps and prioritize its investments to have the most impact on risk reduction.

Maximize the Use of Intelligence

Statistically, an attacker only needs a few hours to obtain a foothold and extract critical data. However, more than 65% of these attacks took months to discover, and most enterprises were informed of the attack from external sources. The core problem is that customers lack a capability to generate and integrate security intelligence effectively. The proper use of intelligence will improve the effectiveness of security operations and increase the speed of response against targeted threats. To efficiently deliver this capability, an organization must understand the intelligence process of collection, integration, and exchange; integrate global, community, and local intelligence sources for full operational capability; and properly employ strategic, tactical, and operational intelligence to maximize decision-making speed.

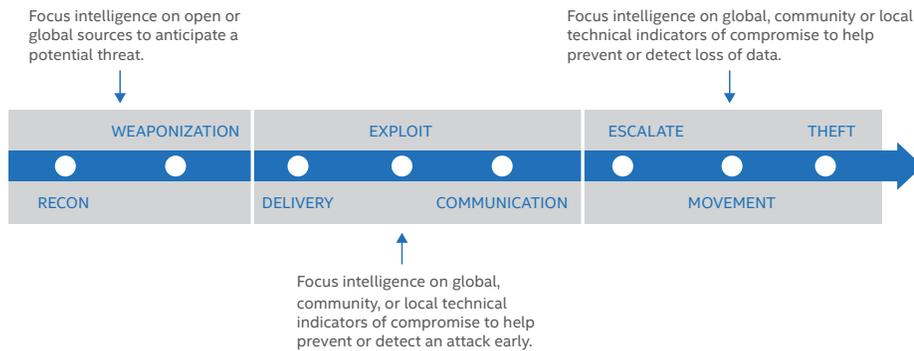
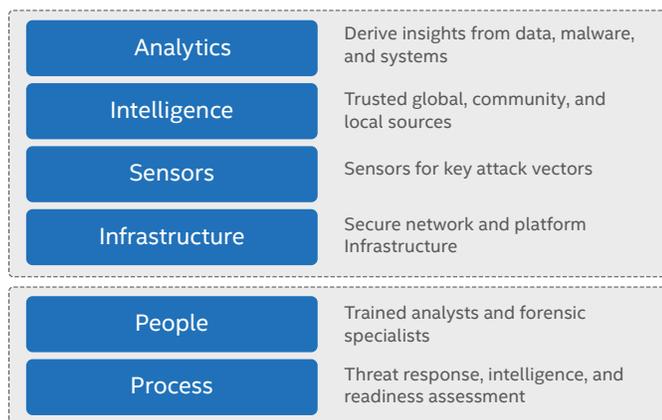


Figure 5. Focusing security intelligence improves security operations and response time.

The above chart represents a potential way to prioritize intelligence investments and integration. Focusing intelligence capability against the attack chain models will maximize effectiveness to identify threats early and reduce the risk to the business.

Continuous Security Operations

Building resilience requires an evolution in security operations capability. At a foundation level of capability, security operation is typically focused on consolidation of security events and developing an initial incident response capability. To address targeted threats, security operations must evolve to a continuous operation that is focused on assessing readiness, acquiring and integrating threat intelligence, and increasing the speed of threat response capability.



Key CIRC Capability Building Blocks

Figure 6. The building blocks of security resilience.

Solution Brief

Increasing the speed and capacity of security operations requires more efficient use of technology to handle complex analytic tasks. Organizations are faced with analyzing millions of security events and suspicious files to find a targeted threat. Often this analysis is manual or short-term, which greatly reduces the scope and speed of the response process. It is increasingly important to fully integrate sensor technology with automated malware analysis capability and intelligence to produce high-fidelity indicators. The more accurate the indicator sent from the sensor grid, the faster security operations can respond to an attack. Automating some of the complex malware analysis tasks will produce valuable intelligence and increase the capacity of security operations to handle more threats. Increasing the speed of response requires having visibility over all the business operating environments and the ability to contain an attack over multiple vectors. Centralizing real-time data correlation and analytics will reduce time to identify and contain an attack while enabling new insights about network, system, and user behaviour that may address other problems.

Summary

Resilience is an evolution, not a single product, process, or technology. Resilience is also business objective. This strategy document defines some the critical building blocks along the journey towards a resilient and trusted digital enterprise. We are in a period of unprecedented change where transformation and the disruption that can arise from it are the new constant. This transformation and disruption are having a profound effect on security perception and architecture within the business. Intel Security solutions can help the digital enterprise manage risk in the cyberdomain by providing balanced controls across business operating environments and increasing the speed and capacity of cyberdefense to manage the risk from targeted threats. By leveraging Intel Security solutions and connected architecture, an organization can improve resilience and confidently move in new business directions.

