DEFENSE IN DEPTH MATURES

Security threats are growing and evolving. Organizations must adopt more stringent protections revolving around defense in depth.

Over the last few years, security risks have grown exponentially. Hackers, attackers and a motley crew of cyber thieves have enlisted far more sophisticated attack methods to put computers and entire networks at risk.

"The world has changed. Organizations are far more interconnected and the potential cost of a data breach is much greater than in the past," points out John Kindervag, principal analyst at Forrester Research.

To be sure, virtually all entities now store an array of data and information online, including healthcare records, credit card data, Social Security numbers and intellectual property. In addition, a growing number of firms operate mission critical systems and sites that must be up and running 24/7/365.

"It is no longer a lone person sitting in front of a computer and trying to hack into systems," warns Robert Shaker, security CTO in the security business practice at Symantec. "There is an entire criminal ecosystem at work."

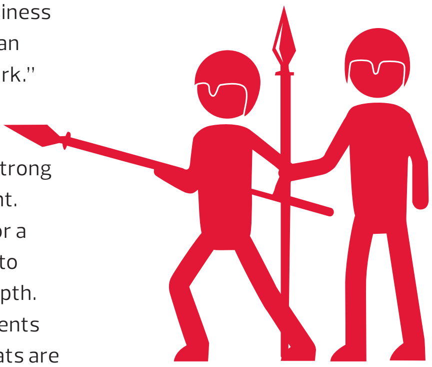
Coping with this new normal is no easy task. Developing an effective strategy and putting strong protections in place is paramount. Today, there's a growing need for a more comprehensive approach to security, including defense in depth.

Enterprise security requirements are changing and evolving, threats are becoming more sophisticated and the damage caused by an attack is more severe. In a worst-case scenario, the damage can be so pronounced that survival is in question.

Today, organizations must focus heavily on four primary areas of defense in depth: gateway and networks, servers, applications and client security. But they must also take a more integrated and data-centric approach to business and protecting assets.

Protection Schemes

The growing complexity of security is forcing many entities and IT leaders to reexamine the way they approach security. According to Ponemon Institute, 90 percent of senior staff say that their organization has dealt with a data breach and half say that they expect more data breaches and breakdowns in the future.



The average cost of a data breach is now $214 per record and about $7.2 million per incident, the research organization reports. Meanwhile, Symantec reports that it processes more than 1.5 billion security alerts daily.

In recent months, attacks, takedowns and break-ins have escalated. Major U.S. financial institutions have faced blistering attacks, several high-profile companies have endured serious security breaches that have revealed sensitive customer data, and government systems have been breached by attackers and gangs with IP addresses originating from outside the U.S.

"Many organizations have done the bare minimum and don't believe that they are a real target," states Jonathan Gossels, president and CEO of SystemExperts, a Sudbury, Mass. security risk analysis consulting firm.

The heart of the problem, security experts say, is that practices haven't kept up with hackers and thieves, who continually devise new and more sophisticated ways to attack networks and steal data. In addition, many breakdowns occur because of lax or poor internal processes.

Workers may eschew rules and procedures or simply not know that what they are doing can add to risk. For instance, a staffer may paste sensitive data into an email or instant message. Or a mobile worker may forego a passlock on a smartphone or tablet. If it's lost, the finder has unfettered access to the device.

Today's bring-your-own-device (BYOD) environment – along with social media and cloud computing – amplifies the risks. Unfortunately, many organizations have struggled to cope with a swift changing environment.

"In many cases, security winds up being like a game of 'whack-a-mole.' Every time you think you have a situation under control and the problem eradicated, something else pops up," explains Deepak Thakkar, director of Data Center Security Product Marketing for McAfee.

Defense in depth is a valid concept, he says. The idea of building layers of protection is the foundation of an effective security strategy.

This includes: gateway and network tools such as antivirus, antispam, content filtering, intrusion detection, firewall, virtual private network (VPN), data loss prevention (DLP) and network access controls (NAC); server security that incorporates authentication, IP security and content filtering; client security that includes antivirus, personal firewalls, threat protection and antispyware; and application security that revolves around effective coding, firewalls and authentication to protect applications and implement strong security policies.

Broad Integrated Solutions

But the concept is evolving away from point products and toward broad integrated solutions. "Organizations require a connected security infrastructure," Thakkar says. "They are recognizing the need to approach security issues in a comprehensive manner.

"This doesn't mean choosing all products and solutions from a single vendor," he says. "The idea is to build a security framework that is cognizant, aware and intelligent. This allows different tools and products within the organization to collect and share information with others."

Within this environment, network security tools gather intelligence as traffic passes through. "The idea is for this information to be shared with systems that are protecting endpoints, such as servers, databases, laptops and other mobile devices – and have some orchestration between all the information. It's not only about having more security, it's about having a more intelligent security posture," Thakkar explains.

This approach means that when a hacker or thief attempts to pry into the network in a different way, the systems can apply previous information to the current situation and recognize there's a problem.

Symantec's Shaker says that as endpoints become more scattered and diversified because of mobility, clouds and other factors, the challenges grow significantly. He suggests that while the need for defense in depth hasn't disappeared and won't fade into history anytime soon, organizations must focus on a more information-centric approach.

"A good security strategy requires ongoing risk assessment," he adds "You can't determine how best to protect systems, devices and data unless you know how it can be misused or compromised."

In fact, Forrester's Kindervag says that organizations must move beyond a model that breaks protections down into individual components and focuses solely on tools. Security now requires a more holistic and conceptual approach.

"There's a need to use discovery techniques to identify important data – toxic data – and then classify, tag and protect it," he adds. "Effective security involves more than protecting networks and devices. It's necessary to build a framework that focuses on guarding the data itself."

Among other things, this means identifying who should have access to specific data and what privileges and rights they have at any given moment. Access controls, encryption and firewalls are key elements, he says.

However, the concept must extend to network inspection of data as well as data retention policies. It also involves understanding ingress and egress points on the network and understanding all vulnerabilities. "Sometimes it's as simple as getting rid of data that isn't needed any longer or using data masking techniques – so-called 'kill data' – in order to strip the value from it in the open market."

>

DEFENSE-IN-DEPTH COMPONENTS

A defense-in-depth solution is designed to minimize risk by adopting a multilayered security solution that protects critical IT data and resources.

Typical components include:

- Antivirus
- Firewall
- Intrusion Detection System (IDS)
- Intrusion Protection System (IPS)
- Encryption
- Automated Patch Management
- End-user Security Training

Getting Defensive

The starting point for building a defense-in-depth strategy is to conduct a thorough analysis — and one that focuses heavily on endpoints. Typically, the task is best left to a third party consultant or firm that can examine network inner workings from the outside in.

Any type of analysis must span departmental boundaries and break down organizational silos. As different units and departments procure and deploy systems — including cloud services — the risk of a gap or vulnerability occurring grows.

Thakkar says that it's critical to approach security from the perspective that various products and solutions must work together seamlessly. "It is important to ask a vendor or consultant how well a product works with other tools and solutions that are already providing different certain defense-in-depth capabilities. If a product doesn't integrate well, you have to ask whether it's worth operating an island of security."

Both McAfee and Symantec offer suites that address many of these challenges. For example, McAfee's Data Center Server Security Suites address a wide range of challenges for databases, servers, hypervisors and virtual desktop infrastructure.

These solutions provide a number of sophisticated and integrated capabilities, including whitelisting, blacklisting, intrusion detection, activity monitoring and virtualization support across physical devices and virtual machines. The suites are tightly integrated with McAfee ePolicy Orchestrator, which provides a security management platform that handles risk assessment, security management and incident resolution.

Symantec's Critical System Protection technology also provides advanced capabilities. It secures both physical and virtual data centers through a host-based intrusion detection system (HIDS) and intrusion prevention system (HIPS). It provides deeper integration with VMware and, among other things, delivers key features such as file integrity monitoring; configuration monitoring; targeted prevention policy controls; granular intrusion protection policies; file, system and admin lockdown tools; and broad physical platform support.

The latter monitors and protects Windows and non-Windows based platforms including Solaris, Linux, AIX, and HP-UX. It also leverages virtual agents for unsupported or less common platforms.

In addition, Symantec offers a number of other tools and solutions that can be used as part of a defense-in-depth strategy. These include: endpoint security — which supports Windows, Mac and Linux — and provides protection against new and unknown threats in virtual environments across numerous endpoints; DLP, which monitors sensitive data across the network and onto devices such as iPad and iPhone devices; reputation-based security that analyzes executable files for 154 attributes and determines whether or not they should run on a particular system; and comprehensive security assessment services.

Shaker says that, in the end, an organization must adopt an approach that provides a high level of flexibility. "The biggest problem today is that attackers change their methods faster than IT shops and the security industry can keep up. They're constantly revamping the way they engineer an attack. They constantly probe for vulnerabilities — and all it takes is getting it right one time to wreak havoc on an enterprise," he says. "Without highly integrated multiple layers of protection, an organization is highly susceptible to a breach."

Forrester's Kindervag says that security challenges aren't likely to disappear. "Hackers don't have change management, they don't have to get approval to try something new. IT decision makers must learn to build a security strategy that's agile and based on connectivity."

For many organizations, he says, it's necessary to make radical changes. "The idea is to make the network a very powerful and scalable enforcement point for data security," he explains. Forrester refers to this concept as a "Zero Trust Model."

Make no mistake, security must now be positioned as core to the organizational function. As data has become digital and systems have become increasingly interconnected, the need for broad and deep security measures has morphed from important to critical.

Says Kindervag: "Attackers have become far more sophisticated. Hackers are bypassing conventional controls that are mostly based on the perimeter. Organizations must get a lot smarter about how they approach security." ■

LEARN HOW CDW DEFENSE-IN-DEPTH SOLUTIONS KEEP YOUR NETWORK SECURE.