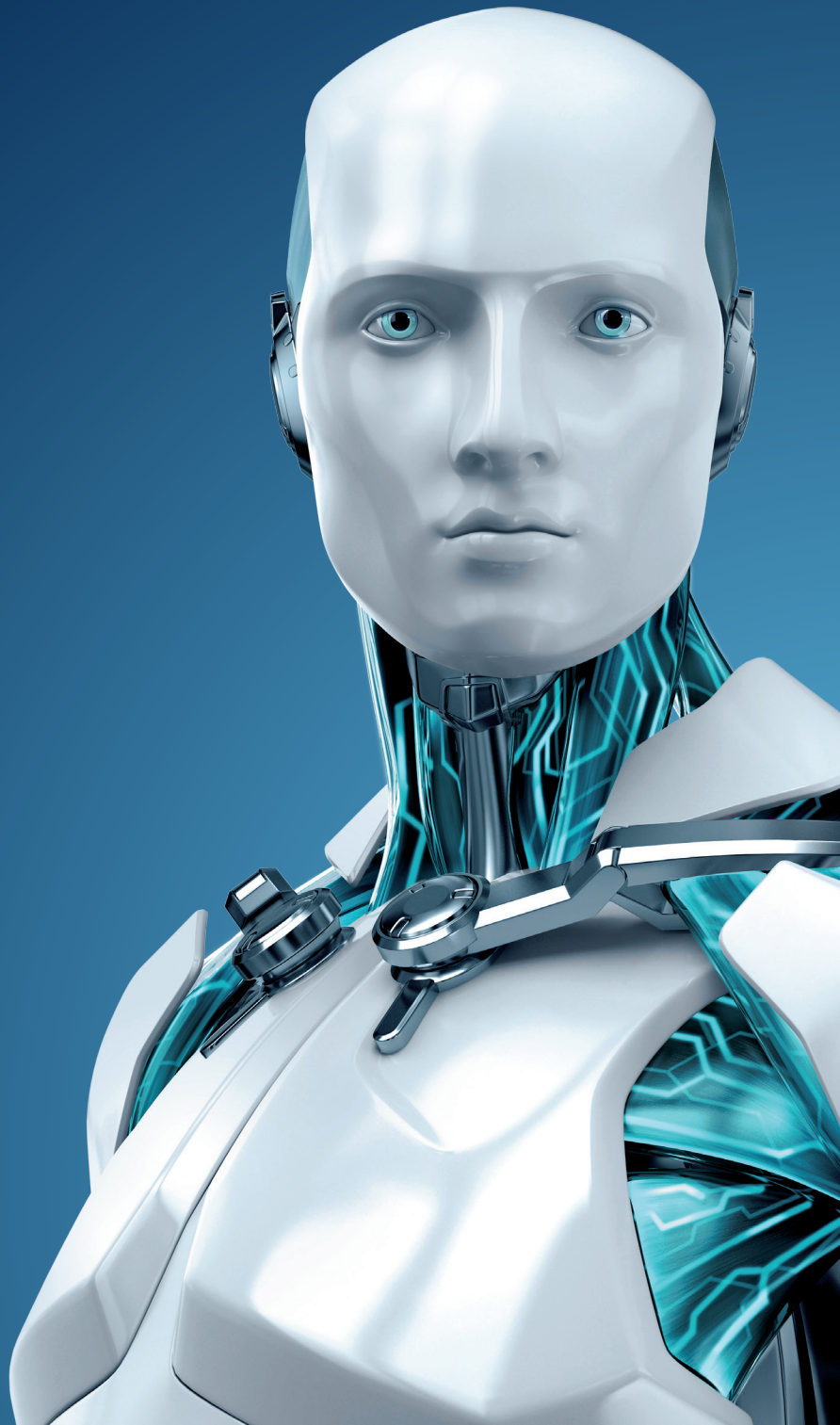
TECH BRIEF

The layered approach to defending your systems and data



ENJOY SAFER TECHNOLOGY™

THE LAYERED APPROACH TO DEFENDING YOUR SYSTEMS AND DATA

By Stephen Cobb, ESET Security Researcher

You only need to visit one medieval castle, or watch one episode of *Game of Thrones*, to understand the concept of layered defense. In days of old, that meant some combination of outer wall, moat, drawbridge, portcullis, inner wall, and keep – all working together to protect the crown jewels from the bad guys.

Today, the crown jewels of your organization are likely to be stored digitally, on a computing device of some kind. We're talking jewels such as secret recipes and product designs, marketing plans and project bids, bank accounts and customer lists. To properly protect these vital digital assets, you need a layered approach, sometimes referred to as "defense in depth."

Let's review the possible layers that can be combined to create strong protection against the growing hordes of bad guys who are trying to steal your secrets, your clients, and your money.

Information Security Policy

You might not think of policy as a defensive layer, but in fact, having a well-rounded information security policy is critical to a layered defense because it embodies your commitment to security and guides the implementation of all the other security layers.

Awareness and Training

Security policies and defensive measures are useless if your employees don't know what threats the organization needs to defend against. There needs to be security awareness for all and security training for those who need cybersecurity skills. All employees don't need to be technical security experts, but they do all need to know that security is everyone's responsibility.

Backups and Continuity

Having all of your files backed up and a copy of that backup stored in a safe place can save the day when all other defensive layers have been penetrated by the forces of evil or even sheer bad luck. Larger organizations should give serious thought to backup facilities as well as digital backups. What if the building AC breaks down or a natural disaster puts the office off-limits? Be prepared to respond with backups and a business continuity plan.

Physical Security

I need an electronic badge and a physical key to get to the workstation in my office (the elevator won't even go to my floor without a swipe of my badge). This is physical security, an important layer of defense that too many organizations overlook. Physical security for your digital devices can be tricky if they are in semi-public places, like a store or restaurant, but not impossible. From security cables to surveillance cameras, there are ways to reduce theft and interference.

Encryption

Even if someone penetrates your layered defense and finds the folder containing your most valuable secrets, a good encryption program will prevent him or her from reading it. Use encryption on all sensitive data, not only when it is being stored on a server, but

also on endpoints such as laptops and in transit such as email (there are encrypted email services available, or you can use encrypted attachments to transmit sensitive data even if the message is not encrypted – just provide the password through a separate channel).

Insurance

Wrapping up your layered defenses is the option to hedge your bets with a cyber insurance policy. They are becoming more widely available and can cover a range of potential problems (for a range of premiums). Check with your business insurance agent for details.

Authentication

If someone sits down at your computer, can they access your files and your network connection? The correct answer is: not without authentication. Everyone using your systems should be accurately identified, preferably via multiple factors, such as a password and a token or fingerprint. And all devices should "time out" and lock when unattended.

Access Controls

Once granted, access to a system needs to be controlled. Unless you are a very small organization that trusts everyone implicitly, you will not want all employees to have equal access to every piece of data. Many organizations create and assign access based on job function or role. Not everyone needs to be able to see bank account balances and personnel files. And of course privileges for anyone who leaves the organization should be terminated immediately.

Filtering and Firewalls

When you surf the web, your browser should be filtering what you see – not censoring websites, but checking pages and links for malicious activity. All of the major browsers do this (Chrome, Firefox, Microsoft IE, and Safari). Where your employees go on the Internet when using company computers should also be filtered based on rules you control. Firewalls can implement rules to control user activity as well as block many different types of attack on your network and devices.

Anti-Malware

Today's anti-malware suites use a wide range of techniques to detect and block incoming code that is malicious, from viruses and worms to Trojans, botnets, and phishing attempts. Don't be fooled by claims that "traditional antivirus doesn't work." All of today's leading antivirus products employ a lot more than traditional technology. The trick is to keep your anti-malware up to date and deploy it across all platforms, from mail and file servers to desktops, laptops, tablets, and smartphones. And don't forget to scan all removable media such as USB flash drives.

Audit and Review

As you may have figured out by now, when it comes to cybersecurity, the defense never rests. Not only do you need to respond to emerging threats, but you also have to periodically check your current layers of defense. Hire a penetration tester to verify that everything is locked down tight. Review security strategy in light of new threats and adjust accordingly.

Monitoring

You cannot maintain the security of a system if you don't monitor it, and that is what logs are for – recording the actions of users based on their authentication to the system (one reason why all employees should be aware that sharing of access credentials is a serious offense). Most operating systems have extensive logging capabilities. Be sure you use them (don't just turn on logging, but check the logs on a regular basis or get monitoring software that will do that for you).

Threat Intelligence

A key layer in the defense of your digital crown jewels is knowledge about who is trying to steal them and the latest techniques that such felons employ. That means staying current with the ever-shifting "threat landscape." While this might sound like a daunting task, your IT security folks can subscribe to intelligence reports, some of which are sophisticated enough to make appropriate adjustments to your security settings as threats evolve.