The Four Pillars of Endpoint Security

DAN GRIFFIN

Copyright © 2013 Daniel C. Griffin
All rights reserved.
ISBN: 1475232705
## Contents of Excerpt

### Overview and Concepts

1. Security is an Advantage .................................. 1  
2. The Four Pillars ........................................... 3  
3. BYOD Security ............................................. 7

### Complete Contents .......................................... 10  

### Author Bio ................................................... 11

1. Security is an Advantage

The Four Pillars of Endpoint Security is a model for making IT security a strategic business asset. Why is this important? Because the most competitive companies want their employees to be productive on their own terms: whenever, wherever, and from whatever device. The best people—the ones you most want to hire and retain—are exactly the ones that are attracted to flexibility, enablement, and rapid decision making.

The most competitive, high-velocity businesses are built on a strong foundation of information technology. IT capabilities, such as providing low-friction access to data and rapid deployment of the latest line-of-business applications, are necessary ingredients, but these capabilities don’t develop overnight. Instead, strategic IT capabilities are created through systematic investment, continuous improvement, and recognizing the strong link between IT and business enablement.

Likewise, strategic IT capabilities are built on a foundation of security. If sensitive data can’t be protected, one of two things will happen. Either the data won’t be made available in the situations where employees are most likely to need it (e.g. on the road, at a customer site, or in a critical meeting), or the data will be made available and it will become compromised or exposed to an unauthorized party. Either way, the business suffers.

The good news is that the tools are available to lay a strong foundation of IT security and to enable the business. The Four Pillars of Endpoint Security provide an easy-to-use context for evaluating and prioritizing the use of those tools.

The Four Tenets of Security

Cloud computing has changed some things like scalability and the cost model for web application hosting. But when it comes to security, the basics still apply. There are four tenets of security: identity, authentication, access control, and authorization.

1. **Identity**—how principals, such as users, are represented.

2. **Authentication**—how identity is established. For example, a user in possession of a smartcard provisioned with a trusted X.509 certificate, plus knowledge of the smartcard PIN, will use the card to authenticate, thereby establishing his or her identity within the system.
3. **Access control**—the ability of the system to selectively allow or deny principals to perform actions on protected objects. Access control enforces authorization rules.

4. **Authorization**—the process by which access control rules are expressed.

To better understand these four tenets, imagine this: Airbus and Boeing are collaborating on a new Joint Strike Fighter (JSF). Rather than exchange huge engineering design documents between worldwide teams every night, which is what projects of that scale used to entail, the teams collaborate by using a more modern and manageable mix of:

- Centralized document repositories, such as SharePoint.
- Security token server, such as Microsoft Active Directory Federation Services (ADFS) or Shibboleth.
- Password-based and multi-factor authentication technologies, such as smartcard or one-time password (OTP).

In the case of identity, within Airbus’ Active Directory (AD) domain, users are represented as security identifiers (SIDs). But those SIDs may have no meaning in Boeing’s AD. So identity might be represented by user email address plus other metadata, such as project group membership. And in the case of authorization, it may be necessary to define authorization rules granting auditing staff read-only access to documents on cost expenditures and accounting staff read/write access to those documents.

In order to support complex, collaborative projects such as a design of a JSF, security software has become increasingly complex. For example, the most sensitive data may only be accessible to users with specified project group membership, with certain national citizenship, and from provably secure client hardware. But how do you define an authorization language that allows such rules to be expressed by a typical system administrator? The rules can get even more complex: suppose Airbus trusts identity data regarding JSF weapon system group membership originating from Boeing, since Boeing is contributing to that system. But claims regarding propulsion system group membership from Boeing must be ignored, since that subsystem belongs to Airbus.

Looking at the current state of the art, the capability of expressing such rules exists in the form of standardized technologies such as SAML and XACML. While some ramp-up is required, especially when it comes to complex collaborations, sophisticated line-of-business application integration with those standards is available.
2. The Four Pillars

The Four Pillars of Endpoint Security complement the four tenets discussed in Chapter 1. The basic premise of the Four Pillars of Endpoint Security is to allow the network to perform even while under attack. But what is an endpoint? In this model, an endpoint is any of the following (where the work is actually done): desktops, servers, and mobile devices.

With these assets in mind, the Four Pillars of Endpoint Security include:

1. **Endpoint hardening**—protect the endpoint from attack.
2. **Endpoint resiliency**—make the endpoint auto-healing.
3. **Network prioritization**—guard network bandwidth.
4. **Network resiliency**—make the network auto-healing.
Endpoint Hardening

The goal of the first pillar—endpoint hardening—is to ensure that network assets are using the latest technologies to defend against threats. Typical threats include unsafe email attachments, worm-like viruses that propagate over the network, and related threats to your web browsers.

One example of an attack counter-measure is the isolation, or sandboxing, of computer application processes from potential malware by way of mandatory integrity levels enforced by the operating system (OS). This type of protection is applied to Google Chrome and Microsoft Windows. However, manageability can be lacking—namely, the ability to centrally deploy and manage isolation settings for the entire host. In order to be useful, this needs to be done in such a way that third-party applications work seamlessly (and are protected).

How does monitoring apply to this pillar? You should monitor network assets for intrusions in the field in a scalable way. You should also watch for unexpected behavior patterns. The following technologies can aid in endpoint hardening:

- Antivirus and anti-malware software
- Mandatory integrity levels
- Auditing of network resource access

Endpoint Resiliency

The goal of endpoint resiliency is to ensure that health information on devices and applications is continuously gathered and monitored. That way failed devices or applications can be automatically repaired, thus allowing operations to continue. The following technologies can make endpoints more resilient:

- Network access control (NAC), including products such as Cisco NAC and Microsoft Network Access Protection
- Configuration baselining, including the use of government standards such as Security Content Automation Protocol (SCAP)
- Patching
- Antivirus and anti-malware software
- Centralized policy and confirmation management, including products such as Microsoft System Center and VMware vCenter
An open area of development in this space is the need to marry these technologies to produce auto-healing behavior based on standardized, easy-to-extend baselines.

How does monitoring apply to this pillar? Consider trends in any of the following areas:

- Which machines are out of compliance?
- In what way are they non-compliant?
- When is this non-compliant state occurring?

All of these trends can lead to conclusions about potential threats, whether an internal threat, an external threat, a configuration error, user error, and so on. Also, when you identify threats in this manner, you can continuously make endpoints more robust in the face of increasingly sophisticated and distributed attacks.

**Network Prioritization**

The goal of network prioritization is to ensure that your infrastructure can always meet application bandwidth needs. This consideration applies not only at well-known peak demand times, but also when there are unexpected surges on network loads and distributed external and internal attacks.

Technologies that can manage application bandwidth include DiffServ and Quality of Service (QoS). However, this pillar currently represents the biggest technology gap between what’s needed and what’s commercially available. In the future, it would help to have solutions to integrate user identity, application identity, and business priorities. Then network routers could automatically partition bandwidth based on that information.

How does monitoring apply to this pillar? Network routers should be doing the flow logging for trend analysis, and effective and comprehensive monitoring can help provide answers to these questions:

- How are today’s flows different from yesterday’s?
- Is there an increased load?
- What new addresses are involved?
- Is the new traffic originating overseas?

**Network Resiliency**

The goal of network resiliency is to allow for seamless asset failover. Techniques in this area ideally afford reconfiguring the network in real-time as performance degrades. This pillar is similar to endpoint resiliency in that the goal is to facilitate network self-healing in order to minimize the management burden.
This pillar also draws attention to the fact that failover and redundancy must be considered on a large scale, as well as a small scale. For example, you can use clustering technology to provide failover of a single node within a datacenter, but how do you provide failover for an entire datacenter or region? And the challenge with disaster recovery planning is broader still, because you must also consider office space, basic services and, most importantly, staffing.

In addition to clustering, other relevant technologies under this pillar include replication and virtualization. How does monitoring apply to this pillar? Failover technologies in general rely on monitoring. Plus, you can use load data for resource and acquisition planning as business needs evolve.

Fulfilling the Four Pillars

For each of these Four Pillars of Endpoint Security, there are likely to be commercially available security, network, and business-continuity technologies that are either underutilized or not yet deployed by most organizations. Thus, you as an IT manager have the following opportunities:

- Use the Four Pillars, or some other framework, to identify threats and gaps in your network defenses
- Make additional investments in automation and monitoring
- Engage more closely with business decision makers on the costs and benefits of these efforts

Some enterprises may already find themselves on the cutting edge of what’s readily available in one or more of the pillar areas. Thus, there are plenty of opportunities for the entrepreneur as well. What is critical is to restructure your thinking to accommodate each of these Four Pillars, as each is essential.
Bring your own device (BYOD) is the trend in enterprise IT to rely on users to supply their own computing hardware in the form of smartphones, tablets, and, to a lesser extent, laptops. While there is an ostensible cost savings to be had in capital expenditure, and businesses can realize productivity in making it as convenient as possible for employees to always be connected, BYOD is mostly just a response to an external reality: as smartphones become more capable, consumers use them for almost all computing tasks aside from heavy content creation (e.g. programming, video editing). Plus, while checking work email can be a primary task for a consumer smartphone, the latest generation of users communicate via SMS, Facebook, and Twitter. All of those communication needs are met using public, free apps.

In that context, providing knowledge workers with a separate, corporatemanaged, mobile computing device is moot. Nobody needs it.

But if your responsibilities include IT security management or compliance, then you should already be squirming. There’s a balance to be struck, and it’s unlikely to be the same for any two businesses. On one hand, you have to support the latest communication, collaboration, and information exchange modalities if you want to attract and keep the best people and stay ahead of your competitors. On the other hand, there is a fiduciary obligation to deploy security control systems that, at minimum, help keep honest people honest when it comes to data storage and exchange.

Recent competition in the mobile sector has really paid off for consumers: the latest devices from Apple, Google, and Samsung are incredibly cutting-edge and also incredibly usable. That impressive combination is in fact an inspiration for us security folks. Heterogeneity is hard for the IT security manager, since disparate mobile platforms expose different security controls. Yet, the raw power and extensibility present in these devices means that the sky is the limit, both for the IT security manager in terms of developing and applying controls, as well as for the business manager in terms of dreaming up new scenarios for increasing business capability and velocity.

So what steps do you need to take to secure all those mobile devices for corporate data access? You can use the Four Pillars of Endpoint Security as a guide.

1. **Endpoint hardening**—technologies like platform attestation allow server-side resources to extract high-assurance security claims from mobile devices. This helps to keep sensitive data off of malware and rootkit infested devices and can also be used to enforce client attributes, such as the use of...
hardware-based disk encryption. The latest generation of mobile devices supports a variety of high-integrity security features, including TPMs, SIMs, and other hardened cryptographic and data protection features.

2. **Endpoint reliability** —the ability to make mobile devices self-healing is still a work-in-progress, but all of the major platforms have recognized the increased support cost, and negative user experience, that comes from supporting a wide-open application ecosystem in which discerning good software from bad is impossible for the layman. Curated app stores help endpoint reliability, although they don’t guarantee it. This is moving in the right direction, but enterprises with sophisticated security needs must still necessarily distinguish between managed (for example, an Active Directory domain-joined laptop) and unmanaged (typical smartphone) devices when it comes to granting information access. Enforcing patching and platform updates is key to maintaining endpoint reliability; technologies exist to do this across all platforms.

3. **Network prioritization** —link encryption is a must-have. All web applications should enforce Transport Layer Security (TLS); all clients support it. Don’t waste bandwidth on unencrypted or untrusted requests.

4. **Network reliability** —many of the same proven security technologies and practices apply equally across traditional enterprise computing assets: routers, servers, laptops, and desktops. Don’t forget that (a) they need to be utilized and (b) they’re constantly increasing in sophistication. This applies whether the assets are mobile, private cloud, or public cloud.

In summary: embrace BYOD, enable your business, and allow your employees to be more productive anywhere and from any device. But don’t forget to do your risk management homework.

### A BYOD Security Cautionary Tale

Never before has the information worker had so much computing power (e.g. smartphone or tablet) always on hand. And never before has it been as easy for IT to support the business with ready access to the data and tools necessary to enable new revenue sources and faster decision making. The decision to embrace BYOD is an easy one: employees, partners, and vendors are likely already using their own computing devices to communicate and collaborate.

But what can be done to establish and enforce practical data security policies for a fast-changing, heterogeneous computing environment? Take a look at this typical BYOD security cautionary tale.

Widget Co. stores its documents on SharePoint and recently migrated to Office 365. The migration has been a boon to the Widgets business teams: they have more control over the look and feel of their team SharePoint pages, they can support a variety of client devices, and allow remote employees, frequent travelers, and vendors to collaborate. Plus, outsourcing is saving time and money for the in-house IT team, allowing them to focus on more strategic efforts, such as enabling new line-of-business scenarios.
Recently, though, a senior executive, distracted after leaving a meeting in a foreign city regarding a potential merger between Widget Co. and Acme, left his tablet in the back of a taxi. Since he’s not sure what documents had been downloaded, or when, it’s tough to assess the potential impact of the unauthorized data disclosure if the device falls into the wrong hands. Either way, the timing of the loss couldn’t be worse: if Acme, its competitors, or even members of the foreign government were to learn details about Widget Co.’s internal discussions about the proposed merger, it could put Widget Co. in a bad place, and likely result in the termination of the executives leading the effort.

**Next Steps for the Business Decision Maker**

What can the business decision maker (BDM) do to avoid this scenario? The first recommendation may come as a surprise, but this is the real opportunity for the decision maker: don’t miss out on the opportunity to enable “anywhere” data access. Wherever your employees happen to be, and whatever device they happen to be using, consider how to let them be most productive. That doesn’t mean throw the barn doors wide open to your most sensitive corporate assets. Instead, it means make a reasonable plan for taking advantage of the latest collaborative tools, cloud services, and the security controls they provide. If you don’t, your competitors will be moving more quickly than you to enable faster decision making, new lines of business, and even attracting better and brighter employees who thrive in a more dynamic environment. First and foremost, the focus of the BDM must be on enabling the business.

The second recommendation is where risk mitigation comes into play: with the business goals in mind, work with your CIO, CISO, and IT team to establish data security policies to enable them. Make sure the basics are being covered: user authentication, authorization, auditing, and data encryption. In other words, who should have access, and to what? How are those rules being verified? And how can we protect sensitive data—whether in the cloud, on premise, on the move, or in the back of a taxi—and still foster a competitive, collaborative environment that keeps us ahead of the competition?

The most competitive businesses are constantly looking for ways to gain new advantage from their existing IT investments. Look to IT security to be a business enabler. The latest enterprise software tools and cloud services enable more sophisticated security controls than any previous technology generation—use them!

**BYOD Security: A Happy Ending**

Returning to the example of Widget Co., suppose these data loss prevention policies are established across all IT applications:

- Data is encrypted at rest and in transit
- All mobile devices require password/PIN unlock

With those policies enforced, the lost tablet of the senior executive is a non-issue, the strategic merger between Widget Co. and Acme stays on course, employees stay productive, and the business prospers!

— End of Excerpt —
Complete Contents

Overview and Concepts
1 Security is an Advantage
2 The Four Pillars
3 BYOD Security
4 Keeping Pace with Mobile Computing
5 Security and the Four Pillars

Endpoint Hardening
6 Trusted Platform Modules
7 Bitlocker Drive Encryption
8 Securing Data with Bitlocker
9 Securing Your Browsers
10 Hardening Mobile Phones
11 Cloud Security and Mobility
12 Hardening with the Firewall

Endpoint Resiliency
13 Reducing Attacks

Network Prioritization
14 Trusted Boot
15 More on Measured Boot
16 Securing Resources

Network Resiliency
17 Network Access Protection
18 Securing Your Passwords
19 One-time Passwords

Conclusion
20 Economics and Risk
21 From Four Tenets to Four Pillars

About the Author
Cloud Security and Control

In any technology domain, security has overhead and costs associated with it, and cloud computing is no different. But cloud computing offers some unique opportunities for organizations to use security as a business enabler. For example, many cloud technologies offer ready support for collaboration with partners and customers.

Likewise, cloud services are being used by IT organizations to support mobile computing, the “bring your own device” trend, and the consumerization of IT. In all of those contexts, security technologies are an enabler.


The Four Pillars of Endpoint Security

Security is an advantage: the Bring-Your-Own-Device (BYOD) trend in enterprise IT has caused users to expect anywhere/anytime access to sensitive data, from any mobile device. But IT managers are nervous about serving sensitive corporate data to devices that lack sophisticated security controls.

By applying the Four Pillars of Endpoint Security, businesses can embrace BYOD, stay competitive and operate without interruption, which leads to higher productivity and business velocity.