THE FOUNDATION OF NEXT-GEN ENTERPRISE SECURITY IS EMBEDDED IN YOUR ENDPOINTS

A Study of Endpoint Security

November 2016

INFO~TECH
RESEARCH GROUP

CONTENTS

THE EVOLUTION OF THE THREAT LANDSCAPE

The emergence of Advanced Persistent Threats (APTs), zero-day vulnerability exploits, and the ever-present threat posed by arguably the most dangerous of adversaries, the organization's own users, continue to poke new holes in even the most well-laid security architectures. While the tools that attempt to keep data and other assets safe are doing their best to keep pace, malicious software, and the people behind it, continue to find ways to avoid detection by, circumvent, or even subvert an organization's perimeter and endpoint defenses.

$4,000,000

Average consolidated cost of a single data breach[1]

As the threat landscape evolved, so too has the scope of what must be protected. For most organizations, an architecture with a single chokepoint where external traffic is funneled through various firewalls and gateways is now a pipe dream. Even the notion of a perimeter that can be defined and defended is quickly being shed. Their reality now consists of distributed endpoints that might be personally owned, un-managed, and/or be connecting to unsecured networks on the regular, but still access corporate networks and assets. This new reality has dramatically broadened the attack surface to the point where the perimeter is simply too fluid to successfully manage using a traditional network security architecture.

The damage that can be done when these security architectures are compromised is well documented, thanks in large part to the high-profile breaches at the likes of Target, Sony, Home Depot, LinkedIn, and countless others. Corporate data assets, personal information, sensitive communications and intellectual property are being stolen every day—sometimes to the fanfare of extensive media coverage, and other times completely unbeknownst to the victimized party.

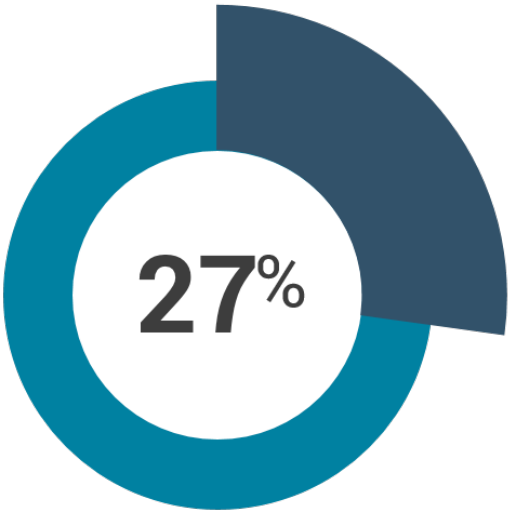
In some cases, organizations are only made aware of breaches impacting them when notified by a third party who has discovered it. In its latest update to the Cost of a Data Security Breach Study the Ponemon Institute[1] determined that the average cost of a single data breach now exceeds $4M (USD), with each record lost costing an organization $158. For many organizations, that could amount to an unrecoverable blow to their bottom line.

[1] 2016 Cost of Data Breach Study: Global Analysis Ponemon Institute (sponsored by IBM), June 2016, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

HOW MUCH RISK IS OUT THERE?

With the level of financial, brand, and in some cases regulatory risk associated with compromised data, it would be fair to assume that most organizations are taking necessary steps to limit their exposure. In today's terms, however, this is no easy task. As the lines between corporate and personal have blurred, or even blended altogether, the enterprise security team has less and less true control over all of the computing assets being used by employees, and the data flowing through those devices. It can be increasingly difficult for the CISO to properly quantify the risk associated with this new reality.

A recent analysis of anonymized data extracted from Absolute's Endpoint Data Discovery solution, conducted by Info-Tech Research Group security analysts, shows that more than one in four devices (27.2%) in the sample contained at least one record containing some measure of sensitive data. This included credit card numbers, Social Security Numbers, or personally identifiable health and financial information. Of even greater concern is that in many cases these devices did not contain one or two records, but thousands, tens of thousands, or even millions of records. At $158 per record, that is an exorbitant amount of risk if even just one of those devices were to be compromised.



More than 1 in 4 devices contain at least one record containing sensitive data

As can be expected, the types of data found on devices corresponds to their industry: devices in healthcare organizations tend to have more personal health information while those devices in the corporate sector trended more heavily towards credit card information. Even within the education sector, where we might not expect to find much sensitive data on endpoints, as many as 42% of devices contain records with some type of personally identifiable information on them. Regardless of the industry, or the specific type of sensitive data, it is clear that there is a lot out there to protect, and even more at stake if that protection falls short.

BUILDING A SECURITY HOUSE

So if an organization can't keep the data off of devices, then what can it do? Info-Tech's information security framework highlights the key technology and governance layers that can be deployed in a structured defense. The framework is laid out as a security house, and much like in an actual home, the assets inside warrant the highest levels of protection. The doors and windows are sealed and encrypted with anti-intrusion measures, the multi-lock system requires coordinated authentication factors, and a surveillance system provides immediate alerts of any incidents or events that indicate a compromise.

These measures (or counter-measures) are designed to work in concert with one another to maximize the enterprise's security posture. With the end goal of allowing devices to have a "trusted" status within the enterprise networks, security technologies attempt to cast this net around both corporate and personally owned devices alike. Like anything in cyber security, though, the constant evolution of threat vectors, malicious tactics, and the ways in which users work continually disrupts even the best security architectures. In some cases, this has reached the point where organizations are adopting a "zero-trust" model, where no action taken by a device is considered trusted until it has been thoroughly vetted and verified.

Zero-trust modeling might sound like an extreme step, but can be rationalized by just how quickly the house can come crashing down due to compromise at the endpoint level:

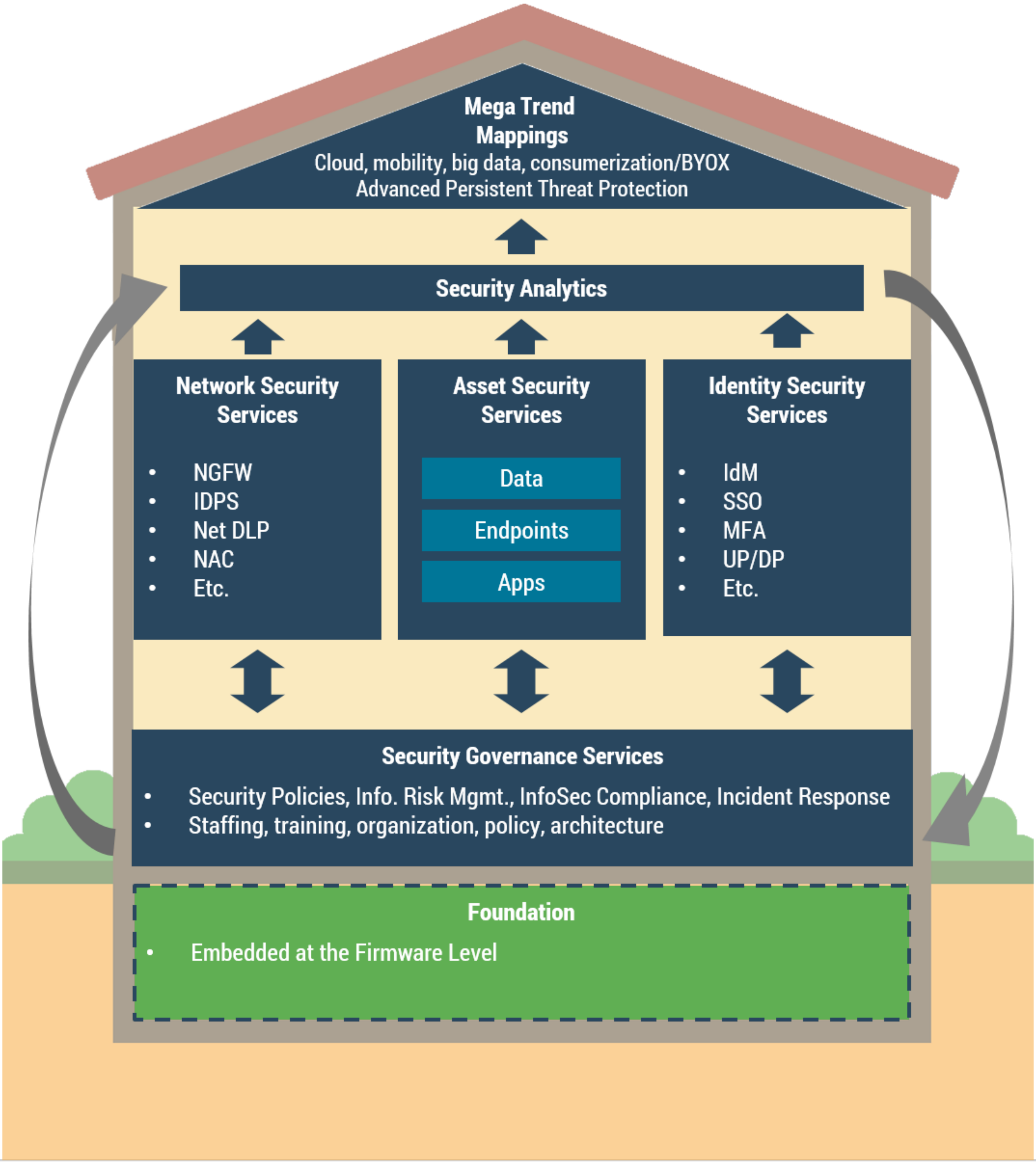
Anti-malware agents can be disabled or uninstalled by various worms or other kernel-level attacks (or an ambitious power user with too much device-level privilege),

Authentication can be gained through brute-force tactics (or spear-phished from those very same users) and,

A lost or stolen mobile device can be taken offline, and side-loaded with various malicious software designed to enable access to the data contained within.

Any structural engineer will know that to keep a real house upright it must sit on a rock-solid foundation, with tie-downs and rebar holding the pieces together. So too can a security house be given that additional reinforcement by integrating it with a foundation that sits below the layers at which malicious attacks happen.

The closer that the security can get to the underlying hardware, the more difficult it is for an attack to successfully compromise. A foundational layer that is embedded at the firmware level, straight from the factory as part of the Original Equipment Manufacturer (OEM), makes the security built on top that much more effective.



Mega Trend Mappings

Cloud, mobility, big data, consumerization/BYOX

Advanced Persistent Threat Protection

Security Analytics

Network Security Services

- NGFW
- IDPS
- Net DLP
- NAC
- Etc.

Asset Security Services

Data

Endpoints

Apps

Identity Security Services

- IdM
- SSO
- MFA
- UP/DP
- Etc.

Security Governance Services

- Security Policies, Info. Risk Mgmt., InfoSec Compliance, Incident Response
- Staffing, training, organization, policy, architecture

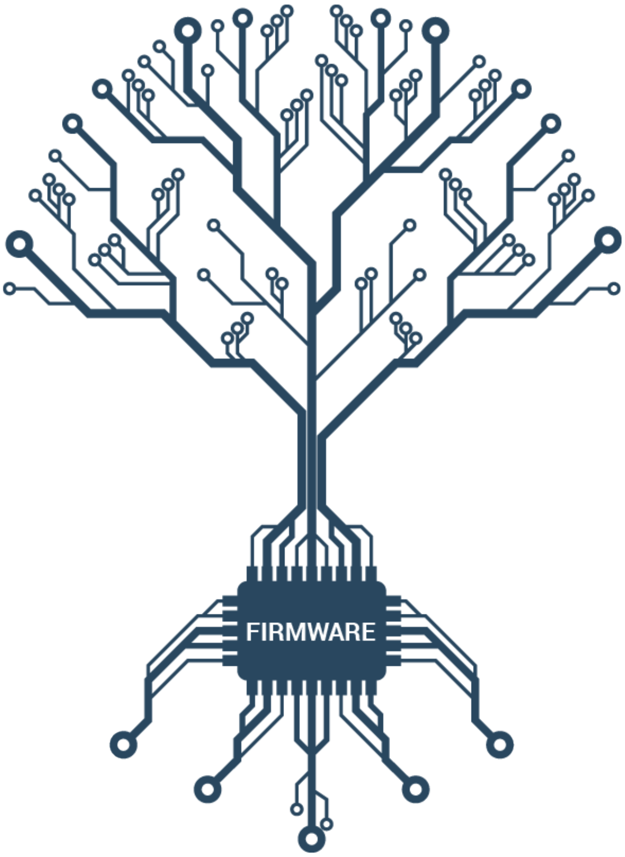
Foundation

- Embedded at the Firmware Level

VALUE OF A SECURE FOUNDATION

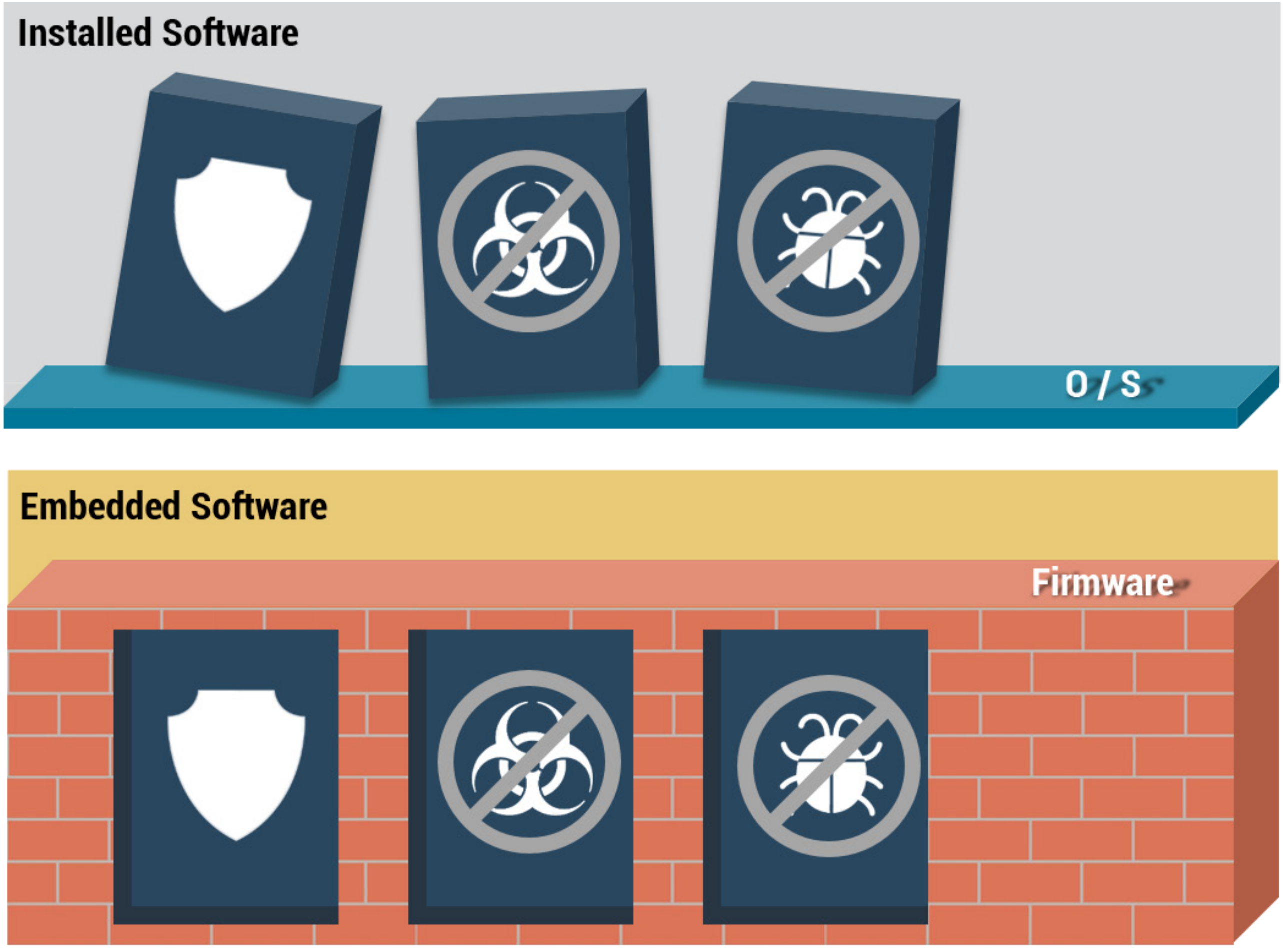
Over the years there have been numerous attempts at pushing security down into the hardware and firmware levels of devices. Some PC manufacturers have attempted to create their own proprietary embedded security, but quickly discovered that in order to be effective, this approach has to be consistent across the entire fleet of corporate devices, not limited to a single manufacturer. In an effort to solve for that distributed requirement, the Trusted Platform Module (TPM) has provided chip-level encryption key storage capabilities on many devices and form factors for over a decade. The module is, however, primarily focused on establishing trust through pre-boot encryption, and not on full device visibility and control.

For organizations with strict controls on personally owned devices and full endpoint lifecycle control and ownership of its corporate devices, TPM can provide an effective foundation through its integration with hard drive encryption and authentication tools. But if a wider variety of form factors must be supported, or if the assets requiring protection may not always be as standardized, then a software solution, embedded at the firmware level directly from the OEM, can offer that broader level of protection.



EMBEDDED VERSUS INSTALLED

It is important to distinguish this type of "software" from the software that is installed in the form of defense agents or monitoring platforms. While the latter can be paused, disabled, or uninstalled with local administrative credentials, an Operating System (OS) reimaging, or a hard-drive reformat, embedded software sits below the OS layer and is protected from these types of subterfuge. Even a factory reset or flashing the firmware to circumvent those factory settings cannot remove some types of embedded software, making them highly resistant to malicious removal. As far as the foundation of a security house goes, this can provide fallout shelter-like strength.



So where does the embedded software fit within a security architecture? How can it be used to bolster the rest of the technologies in place? There are several capabilities which differentiate the embedded endpoint security tools from installed software:

1 SUPPORTING THE REINSTALLATION OF ITS AGENT IN THE EVENT OF DISRUPTION

An attack might compromise the installed agent on a computer in order to begin executing its commands. The embedded component, however, would detect the removal and be able to reinstall that agent, ideally without human intervention.

2 ENABLING OTHER TECHNOLOGIES TO BE AUTOMATICALLY REINSTALLED

Other security tools such as anti-malware, vulnerability management, or configuration management that deploy agents onto endpoints can be bolstered by an embedded solution. Where the necessary connectivity is present, the deployment packages can be initiated and the necessary agents reinstalled when required.

3 REMOTELY ADMINISTER DEVICES EVEN IF THEY ARE COMPROMISED

Enterprise Mobility Management/Mobile Device Management technologies provide varying levels of control and protection to mobile devices, but at their core those devices are still managed by their OS (Apple, Google, Windows IDs). In the event of a boot kit/root kit or another type of device reset, only an embedded technology will be able to continue to provide control to the organization.

4 ACTIVE ALERTING, REPORTING, AND ANALYTICS

There is often not enough value attributed to the data and information collection and analysis that can be done by intelligent security software. Understanding not just the levels of data exposed, but also the types, timing, and frequency of compromise attempts, can enable an organization to start taking proactive action, rather than simply defending in a reactive model.

ACTIVATING THE FOUNDATION

As is indicative in the terminology, embedded security does not need an extensive architecture evaluation or compatibility check because it is already there, waiting to be activated. Once an organization reaches an agreement with the vendor, the dormant module can be activated remotely and begin to perform its security functions. Whether that requires downloading an agent, performing imitation scans, or establishing policies and configurations, the existing presence significantly reduces deployment time and effort.

While the activation process can be much more streamlined than a traditional plan and deploy process, it is still important not to overlook that this new layer will still have to work with other security measures to ensure complete protection. Info-Tech recommends that these key considerations be part of any embedded technology roll-out:

1 WHAT OTHER TECHNOLOGIES ARE TIED INTO THIS LAYER?

If automatic re-installation is going to be one of the key functions, then it is important to gather the requirements and test that the configured policies will trigger on the right events. Where multiple technologies are involved, ensure that a reinstallation of one will not cause conflict with another that is still running.

2 WHAT TYPES OF DATA EXCHANGE WILL THE NEW LAYER BE PART OF?

If there is a SIEM or other monitoring appliance or service in the existing security architecture, then it is critical to check for compatibility with the data that will be generated by the embedded layer. A SIEM is only as good as the data feeds that it ingests: the more data it can analyze, the better it can understand and predict anomalous events across the environment.

3 HOW WILL THE NEW LAYER BE MANAGED?

Nothing in a security portfolio should be taken for granted, so the visibility, alerting, and action protocols must have clear owners and processes to ensure that the solution operates as intended and provides the value that is expected from it.

Just as virtualization, and now containers, have changed the paradigm of how workloads are deployed in a server environment, so too has embedded software changed the paradigm of where security can be deployed on an endpoint. Where the security tools used to build an organization's security house were once limited to above-ground installation, the capability to add a subterranean layer below the application, OS, and accessible firmware levels, offers the most grounded and stable layer of defense. Make no mistake, embedded security does not guarantee that an endpoint cannot be compromised, but its presence has the ability to bolster every layer of security that protects that device, and provide an organization the maximum level of control of the endpoints in its environment. Protect the endpoints, protect the data, protect the house.

About the Author

Elliot Lewis is Vice President of Info-Tech Research Group's Security, Risk, and Compliance Research Practice. Elliot provides thought leadership to the security analyst team, owns the research agenda, and provides strategic guidance to clients.

Elliot has over 25 years of executive management experience, most recently as the Chief Security Architect at the office of the CTO at Dell. Elliot also worked as the Director of Strategic Services, Security, and Identity at Cisco Systems, was Chief Information Security Officer (CISO) of Merrill Lynch, and former Senior Security Architect, Security Center of Excellence for Microsoft.

About Info-Tech Research Group

With a paid membership of over 30,000 members worldwide, Info-Tech Research Group (www.infotech.com) is the global leader in providing tactical, practical Information Technology research and analysis. Info-Tech Research Group has an eighteen-year history of delivering quality research and is North America's fastest growing full-service IT analyst firm.

About Absolute

Absolute provides persistent endpoint security and data risk management solutions for computers, tablets, and smartphones. The solution provides a unique and trusted layer of security so that IT can manage mobility while remaining firmly in control. By providing a perpetual connection with all devices, IT can secure endpoints, assess risk, and respond appropriately to security incidents.

INFO~TECH
RESEARCH GROUP

ABSOLUTE™