FOR MORE EFFECTIVE ENDPOINT SECURITY, IMPROVE YOUR ENDPOINT MANAGEMENT

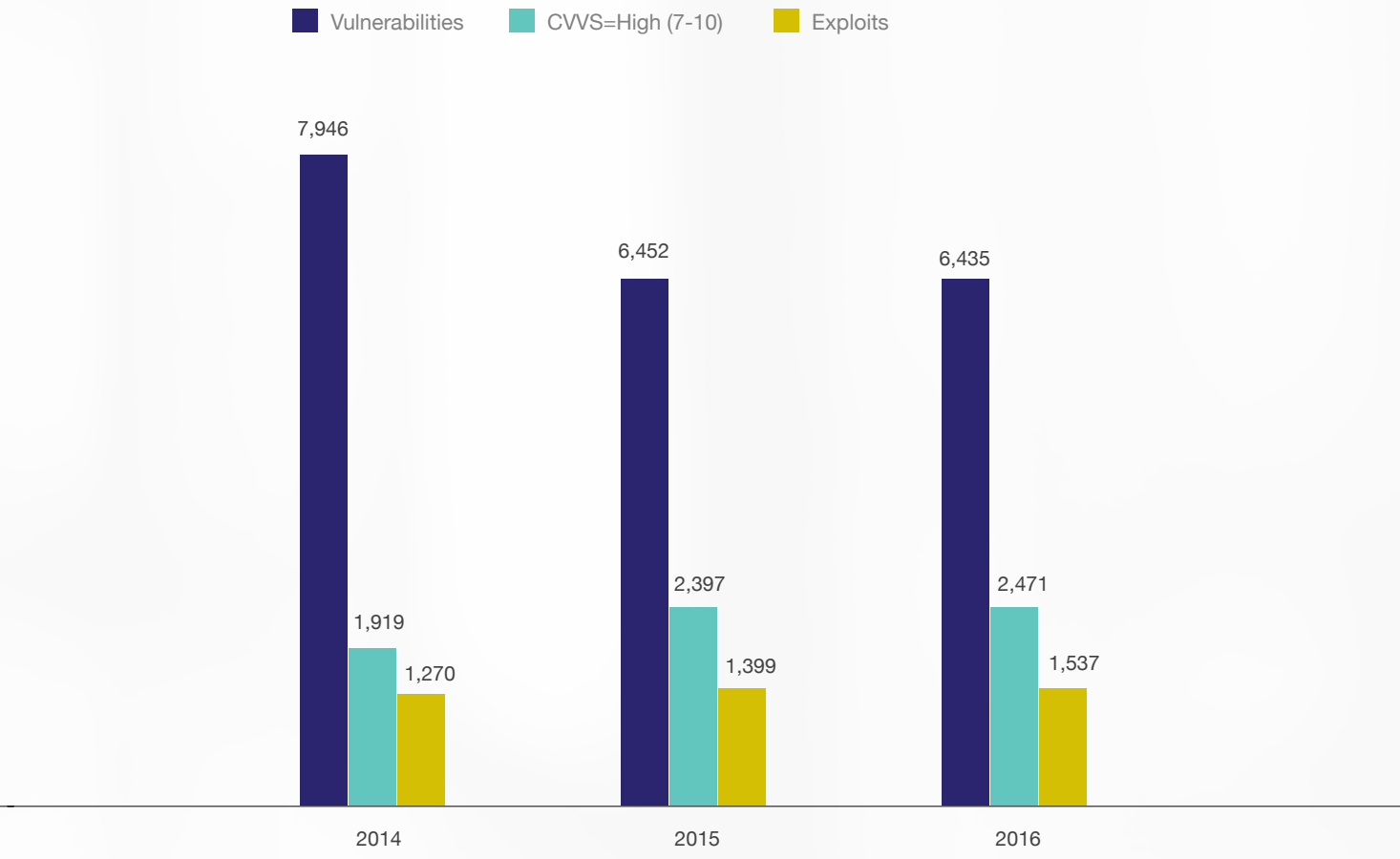
ABERDEEN | LogMeIn

Context: The Current, Ineffective State of Endpoint Security

The current state of endpoint security is a “good news / bad news” situation. The good news is that in recent years there has been a modest trend towards fewer **vulnerability disclosures**, meaning slightly fewer potential ways for computing infrastructures to be exploited. The bad news is that an increasing percentage of vulnerabilities are deemed **critical**, and a growing percentage of vulnerabilities are being **exploited** (see Figure 1).

High-severity vulnerabilities grew from 24% of all vulnerability disclosures in 2014 to 38% in 2016. Over the same period, the number of **exploits** as a percentage of vulnerabilities grew from 16% to 24%.

Figure 1: An Increasing Percentage of Security Vulnerabilities are Deemed Critical, and a Growing Percentage are Being Exploited.



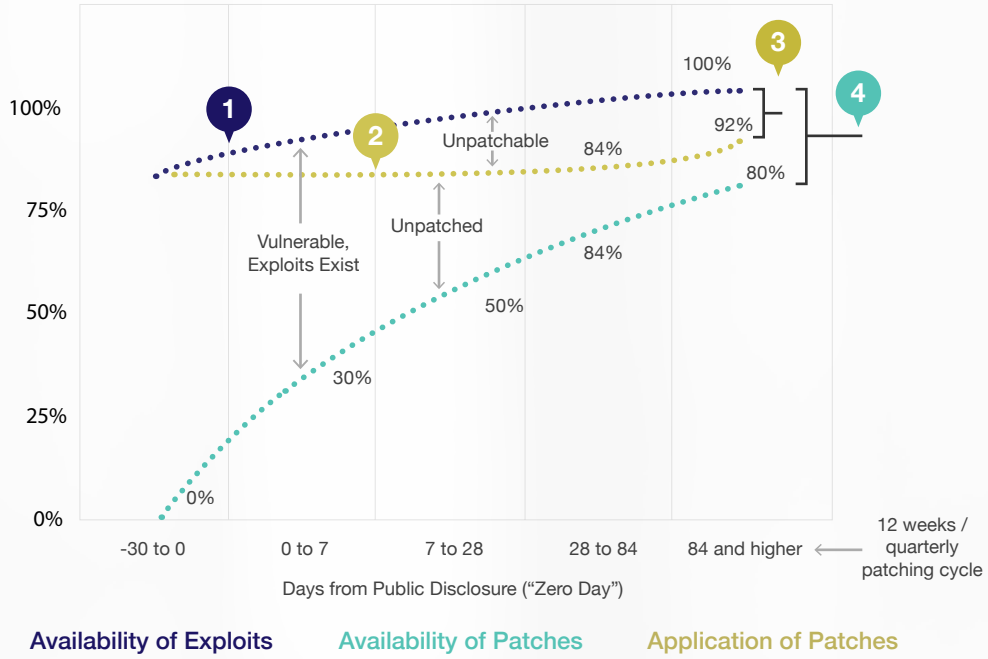
Adapted from cvedetails.com, exploit-db.com; Aberdeen Group, September 2017

Everyone Knows That Proactively Managing Endpoints is "Best Practice" – Right?

Today's endpoint infrastructure is shockingly complex. Aberdeen's simple analysis shows that in a typical endpoint infrastructure with 1,000 users, there are between 50K and 480K changes (e.g., patches, updates, configuration changes, installations, de-installations) made — or potentially made — in any given month, with a median of 250K.

Given the current context, it's no surprise that proactive endpoint management is generally accepted as "best practice." But this is easier said than done. For corporate endpoints, the race of managing vulnerabilities, exploits, and patching is never-ending (see Figure 2):

Figure 2: Managing Vulnerabilities, Exploits, and Patching for Enterprise Endpoints, is a Never-Ending Race — and in General, Unwinnable.



1. **Nearly all** exploits are generally available before or soon after the public disclosure of vulnerabilities.
2. **80-85%** of all vulnerabilities have vendor-provided patches available at the time of public disclosure.
3. After 90 days (i.e., a quarterly patching cycle), about 8% of known vulnerabilities have no patches available.
4. After 90 days, **about 20%** of known vulnerabilities remain unpatched, based on current endpoint management practices.

At This Point, Security Professionals Need to Communicate Effectively with Senior Business Leaders About Risk

As described, the current state of endpoint security is ineffective — which calls for a change in the way endpoints are managed. Challenges of **complexity** and **time** are rendering traditional approaches to endpoint management no longer able to provide effective protection against the full spectrum of **security**-, **operational**-, and **compliance-related risks**:

SECURITY RISKS:

Traditional, signature-based anti-virus / anti-malware solutions are no longer sufficient to protect against endpoint security-related risks.

OPERATIONAL RISKS:

The never-ending treadmill of patch management and configuration management activities are not keeping pace with the timeline of attackers and exploits. For many organizations, limited bandwidth and expertise of available IT staff exacerbates the ability to address these operational needs.

COMPLIANCE RISKS:

Achievement and ongoing demonstration of compliance with regulatory requirements and service-level agreements is still another essential dimension of effective endpoint management that must be addressed.

To *quantify* the security-, operational-, and compliance-related risks associated with current practices in endpoint management, Aberdeen's Monte Carlo analysis models the likelihood and impact of endpoint-related risks as a function of **industry, number of endpoints,** and **number of data records**. In Table 1, the results of Aberdeen's analysis are summarized for the Accommodation and Food Services and Retail industries. These two specific industry sectors leverage endpoints like point-of-sale systems, terminals, and kiosks, which are widely decentralized and inconsistently managed - keeping them squarely in the crosshairs of attackers: **Accommodation and Food Services** and **Retail.** The empirical data shows that this is particularly true for smaller organizations (e.g., 1K or fewer endpoints), which have a higher likelihood of a successful data breach than larger organizations.

Table 1: Quantifying the Annualized Likelihood and Impact of Endpoint-Related Risks in Accommodation and Food Services; Retail (1K Endpoints, 100K to 1M Records).

Annualized Likelihood and Business Impact	Accommodation and Food Services	Retail
Upper Bound (10% likely to exceed)	$11.9M	$8.6M
MEDIAN	$1.67M	$1.25M
Lower Bound (90% likely to exceed)	$100K	$75K

The median annualized business impact from endpoint-related risks is split between the cost of a data breach (about 60%) and the cost of productivity losses (about 40%), with some variation by industry sector.

How Improving Endpoint Management Can Help to Reduce Endpoint-Related Risks

Within a quarterly patching cycle, the empirical data shows that current endpoint management practices leave **about 10%** of endpoint-related vulnerabilities unaddressed — an amount which is about **three times higher** in Accommodation and Food Services (28%) and Retail (33%). Four ways that leading endpoint management solutions can help to address these risks: by **conquering complexity, reducing operational time and cost,** and **reducing the risk of security-related incidents** and **non-compliance issue**s (see Table 2).

Table 2: How Leading Endpoint Management Solutions Can Help

CONQUER COMPLEXITY

STATUS QUO

- Growing complexity of endpoint infrastructure
- Overwhelming number and speed of patches, updates, and configuration changes
- Current approaches to endpoint management cannot keep up

WITH EFFECTIVE ENDPOINT MANAGEMENT:

- Streamline, consolidate, and centrally manage updates to your endpoint systems, saving time and cost
- Reduce productivity loss for users
- Increase productivity of existing technical staff

REDUCE OPERATIONAL TIME & COST

STATUS QUO

- Current approaches to patching and updates are slow and subject to error, leaving endpoint infrastructure vulnerable
- Lack of visibility into endpoint health
- For industry sectors with highly decentralized sites and systems (e.g., hospitality, retail), the time and cost of a manual approach is ineffective

WITH EFFECTIVE ENDPOINT MANAGEMENT:

- Schedule and automate patches and updates to your endpoint systems, to address vulnerabilities faster and more reliably
- Maintain visibility into the success or failure of patches and updates, with robust reporting
- Maintain control over your endpoint infrastructure, regardless of network topology

REDUCE THE RISK OF SECURITY-RELATED INCIDENTS

STATUS QUO

- High likelihood of security-related incidents, resulting in material business impact from data breaches and the time and cost to respond, remediate, and recover

WITH EFFECTIVE ENDPOINT MANAGEMENT:

- Reduce the likelihood of security-related incidents, and their associated business impact

REDUCE THE RISK OF NON-COMPLIANCE ISSUES

STATUS QUO

- High likelihood of non-compliance issues, resulting in the material business impact from the time and cost to address
- Failure to meet requirements of regulatory compliance and service-level agreements
- Difficulty demonstrating compliance (e.g., reporting)

WITH EFFECTIVE ENDPOINT MANAGEMENT:

- Reduce the likelihood of non-compliance issues, and their associated business impact
- Achieve and sustain compliance with regulatory compliance requirements and service-level agreements
- Demonstrate compliance more easily for regulators, auditors, and customers

To learn more, read the full report,
Endpoint Management Risk

LEARN MORE

Created by Aberdeen Group. Brought to you by LogMeIn