Dear Fellow Security Professional //

As a security provider, we understand that convincing executives to make changes to their stack can be difficult. It’s important to clearly demonstrate return on investment (ROI) for any security build out, so that your team becomes more effective with every dollar committed.

It’s important that you—as a critical part of your organization’s security—are able to explain the importance of evolving with an ever changing threat landscape to the people tasked with keeping your organization safe and productive. This can be anyone from an IT leader to a company executive or members of the board.

Our hope is that this document will consolidate the effort required to build out a business case for your organization’s investment in strong endpoint security. The following includes quotes, data points, and industry benchmarks from third-party reports, as well as VMware Carbon Black’s own original data. The result of this effort is a collection of key facts and arguments to help you convince your boss that an investment in endpoint security will be beneficial for your company.

At the end of this document are key steps to help you build your case as well as access to the reports referenced. We hope this information helps you—whether you use it anecdotally or in a formal presentation—to start a conversation about increasing your investment in endpoint security.

Signed,
The VMware Carbon Black Team //
The first step in convincing your superiors to invest in advanced endpoint security is to convince them of the increasing threat to your organization. VMware Carbon Black’s 2019 Global Threat Report\(^1\) stated that 2018 was “The Year of the Next-Gen Cyber Attack.” The authors of the report gave it this label because of the high prevalence of advanced attack methods being used by adversaries that allow them to remain undetected by traditional AV.

ATTACKERS MOVE TO BIGGER TARGETS
According to our data, nearly 60% of attacks now involve lateral movement. This means that once adversaries are in your network, they use that infiltration to move to additional targets. They accomplish this using non-malware / fileless attack methods that use known-good tools within your network.

Additionally, the Global Threat Report indicates that 50% of cyber attacks today leverage island hopping. Island hopping is when attackers target a small company with a more immature security posture because of its affiliation with a larger company that is their ultimate target. They use the first company’s network to infiltrate the second. To combat this, security teams must have a broader focus on the data throughout their organization’s supply chain.

ATTACKERS GOING FOR THE LONG PLAY
Attackers are now executing longer-term campaigns. The Global Threat Report states that 51% of Incident Response (IR) professionals see counter incident response techniques being used during engagements. Verizon’s latest Data Breach Investigations Report\(^2\) corroborates this, stating that 68% of attacks in 2018 went undetected for months or more. The Ponemon Institute reports that this number is even higher. In the study of 477 companies for its annual report on the cost of a data breach\(^3\), the institute found the average time to identify a malicious attack was 221 days and that it took another 81 days to contain it.

ATTACK FREQUENCY AND DAMAGE INCREASING
The Ponemon Institute also states that the average global probability of a material breach in 2019 and 2020 is 27.9%, an increase over last year’s 27.7%. Additionally, the VMware Carbon Black Global Threat Report shows that the average endpoint can expect to see 2 attacks per month in 2019.

Making matters worse, many of those attacks have destructive intent. According to the Global Threat Report, IR firms are now encountering destructive attacks during 32% of investigations. And the damage is costly. The Ponemon study showed a 6.4% annual increase in the average cost of a breach bringing it to $3.86 million.

\(^1\) Global Threat Report: Year of the Next-Gen Cyberattack
\(^2\) 2014 Data Breach Investigations Report
\(^3\) 2018 Cost of a Data Breach Study, Global Overview
The good news is that investing in advanced endpoint security significantly reduces both the probability of a breach as well as the cost impact to an organization if a breach should occur. In the latest Cost of a Data Breach Report from Ponemon, a specific correlation was found between advanced endpoint security solutions and the reduction of the risk and cost of a data breach. The report specifically calls out three functional areas to look at: identification, containment and automation.

**THE 3 FUNCTIONAL AREAS TO INVEST IN FOR COST SAVINGS**

- **IDENTIFICATION** // “The failure to quickly identify the data breach leads to higher costs. Having tools that heighten detective or forensic capabilities can significantly reduce data breach cost.” By how much? The report shows that a breach identified in less than 100 days costs $1.1 million less that a breach identified in more than 100 days.

- **CONTAINMENT** // “The failure to quickly contain the data breach will lead to higher costs. Having tools and processes that heighten remediation capabilities, such as a fully functional incident response process can significantly reduce data breach cost.” By how much? The report indicates that a breach contained in less than 30 days costs $1.16 million less than a breach that takes longer than 30 days to contain.

- **AUTOMATION** // Ponemon refers to security automation as “security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. Such technologies depend upon artificial intelligence, machine learning, analytics and orchestration.” When looking at this factor in the data analysis, “having security automation fully deployed significantly reduces the average cost of a data breach by $1.55 million.”
SPEED AND OPERATIONAL ALIGNMENT REDUCE COSTS

Fundamentally, all of the data points toward speed in accurately identifying and containing issues. A basic concept to ensure your boss understands is that the faster you can find evil and resolve it, the more money you will save. This speed comes from having advanced endpoint security that can provide visibility into endpoint activity and intelligently alert you to potential threats before they become a breach.

Jon Oltsik, Senior Principal Analyst and ESG Fellow states in a recent ESG report on endpoint security that in order to defend against advanced attacks, “organizations need a comprehensive endpoint security technology architecture that is designed for advanced prevention, strong incident detection spanning the “kill chain,” and features/functionality for incident response.”

Real-time query and remediation capabilities are also a must-have according to ESG. With these tools, security analysts and IT operations teams can work together to support incident response. Oltsik advises that advanced endpoint security “can help improve security efficacy, operational efficiency, and business enablement.” This unification of tools and data also serves to streamline remediation steps and provides consistent reporting. Oltsik states this visibility is “a capability CISOs will appreciate as they report on business and IT risk to C level executives and corporate boards.”

CRITICAL CAPABILITIES FOR DEFENDING AGAINST MODERN ATTACKS

Your boss will no doubt want to know you’ve done the research and have a clear understanding of what functionality is needed to defend against modern attackers. Using data from the SANS annual survey on endpoint protection and response as well as their guide for evaluating next-gen endpoint security and their guide for replacing AV, we have compiled a list of the most critical capabilities companies should have to handle next-generation threats.

SANS’ 12 KEY CAPABILITIES FOR DEFENDING AGAINST MODERN ATTACKS

1. Minimize false-positive events, which happen when the product blocks access to a legitimate program.
2. Provide protection, including identification of new, potentially malicious, behavior, with minimal impact on the endpoint user experience.
3. Prevention that stops all types of modern attacks, not just malware; ability to recognize and kill patterns of malicious behavior.
4. Access to multiple forms of prevention, including ability to set different policies for different endpoints, such as remote workers.
5. Provide ability to create, test, and quickly deploy policies to improve prevention and reduce false positives.
6. Pull threat intelligence from multiple sources into a cloud-based intelligence and analytics engine; use this intelligence to identify malicious behavior and increase endpoint protection.
7. Build and customize queries and reports related to endpoint state and activity across the entire organization.
8. Reveal the full chain of processes affected by the malware/malicious behavior.
9. Provide visualization tools, using both graphical and plain language presentations for real-time visibility and retrospective analysis of events.
10. Standard and custom integrations with third-party products.
11. Consolidated cloud-based management console for all modules.
12. Simple deployment, supporting both manual and automated methods of endpoint deployment.
Clear Monetary Value from Investing in Advanced Endpoint Security

ADVANCED ENDPOINT SECURITY REDUCES RISK
Forrester recently released a Total Economic Impact (TEI) report evaluating the results of seven companies who invested in advanced endpoint security. This analysis proved that having advanced endpoint security, which includes predictive analytics, customizable policies, and continuous offline protection, reduced the risk of breach by 20 percentage points. Being able to reduce the average risk from 30% to 10% is a big win for security leaders to report up to executives.

REDUCING COSTS WHEN BREACHES HAPPEN
The biggest cost savings found in the Ponemon Institute’s study was that the average cost of a data breach ($3.86M) goes down significantly when security automation is fully deployed. For those organizations, the cost is reduced to $2.88 million. On the flip side, if a company has no security automation, their estimated cost of a data breach goes up to $4.43 million. That’s a net cost savings of $1.55 million per data breach by investing in security automation.

We used to only see a snapshot of what happened. I didn’t know I needed it [visibility] until I saw it. Now I would never want to try and secure an environment without this level of visibility.

SECURITY MANAGER // MEDICAL DEVICES
FORRESTER TEI REPORT

Dealing with one console and one product makes management much easier. Something used to trigger in our AV. We’d whitelist it, only to see it hit in our antimalware software. Those situations are gone now.

VP IT SECURITY // FINANCIAL SERVICES
FORRESTER TEI REPORT

Our average total cost has increased but we don’t look at these increases as necessarily bad. We are investing in the protection of data for the long term because we know data breaches are not going away.

IT SUPERVISOR // INDUSTRIAL
PONEMON COST OF DATA BREACH REPORT

Data from Ponemon report showing that security automation reduces the cost of a breach
Advanced Endpoint Security Impacts
8 Factors of Breach Costs

Ponemon found a total of 22 factors that impact the cost of a data breach. Having advanced endpoint security in place strongly impacts more than a third of these factors.

1. INCIDENT RESPONSE TEAM
   while you can have an IR team in place without an advanced endpoint security solution, you can better realize the cost-reducing benefit by equipping them with tools that allow them to identify and contain threats faster.

2. EMPLOYEE TRAINING
   when you consolidate your security stack with a cloud-based platform, you’re reducing the number of solutions that you need to train new team members on. Getting new analysts on-boarded quickly and retaining that talent adds cost savings.

3. PARTICIPATION IN THREAT SHARING
   advanced endpoint security facilitates this in three ways: 1) with threat research from professional threat hunt researchers, 2) with the collection and sharing of information discovered by the threat hunting community and 3) security solution providers can use this data to uncover new threats more quickly and build/deploy detection techniques much faster.

4. ARTIFICIAL INTELLIGENCE PLATFORM
   machine learning is a keypart of advanced endpoint security as it is used to prevent and detect potential threats.

5. USE OF SECURITY ANALYTICS
   some of the more advanced endpoint security solutions can analyze more than 1.75 trillion security events daily. Collecting and analyzing all endpoint data, whether it is good, abnormal, potentially suspicious or definitely malicious is key information to provide the historical context needed to understand and contain behavior.

6. CONSULTANTS ENGAGED
   the big cost here is engaging consultants in an emergency situation. When you have advanced endpoint security and access to threat intelligence from the larger community, engaging outside consultants when a breach occurs is on an as needed basis. If it is necessary, it can be done cost-effectively with consultants within the ecosystem of your security solution provider.

7. RUSH TO NOTIFY
   with advanced endpoint security, you catch anomalies earlier and have the full context to remediate faster and more thoroughly than you would otherwise. This gives security teams a much needed time buffer to get a handle on the situation and not rush communications.

8. COMPLIANCE FAILURES
   advanced endpoint security meets the compliance requirements to replace traditional AV. It also provides visibility (notably through live query) to prepare for and prove compliance with whatever regulations are needed.
The impending cost of a data breach that hasn’t happened yet can sometimes be hard to grasp. Forrester’s TEI report addresses this by looking at both the cost of investing in advanced endpoint security as well as the benefits. In doing so, the report calculated that the companies studied saw a 261% ROI and total 3 year benefits of $3.7M.

While the avoided costs of a data breach are significant, the day-to-day resource savings are very tangible benefits for you to show your superiors. Regardless of a data breach occurring, security and IT operations teams will be able to streamline their activities and their their tool sets with advanced endpoint security. All together, these time savings add up to over $2M.

**Financial Summary**

- **Total Benefits PV, $3.7M**
- **Total Costs PV, $1.0M**
- **Avoided Costs of a Data Breach, $1.6M**
- **Time Savings from Faster Investigation & Remediation, $1.2M**
- **Time Savings from Less Frequent Reimaging, $333.9K**
- **Cost Savings from Simplified Operations, $474.4K**

**Benefits (3 Year)**

- **Year 1**: $1.6M
- **Year 2**: $1.2M
- **Year 3**: $333.9K

**Forrester Total Economic Impact - Results of Investing in Advanced Endpoint Security**

**HOW THE TIME SAVINGS ADDS UP**

**TIME SAVINGS FROM FASTER INVESTIGATION** // Effective prevention and detection, comprehensive endpoint visibility, and intuitive attack visualizations reduce the time required to investigate and remediate - saving four hours per event per day. A common number of daily events for an organization to experience is six. However, larger organizations may experience upwards of 40 events per day; which would equate to time savings of 160 hours per day.

**COST SAVINGS FROM SIMPLIFIED OPERATIONS** // Consolidating to a single agent and shifting to a cloud deployment saved two full time equivalents (FTEs) per year - eliminating the inefficiencies of maintaining on-premise security solutions like legacy AV, antimalware and EDR solutions.

**TIME SAVINGS FROM LESS FREQUENT REIMAGING** // Real-time investigation and remediation reduced the need to reimage machines by 90%.
BUSINESS IMPACT

Time Savings & Increased Visibility Provide Business Value

Security and IT professionals are bogged down detecting and responding to potential threats. They need solutions that collect endpoint activity data, detect and prevent suspicious behavior, and facilitate a faster response.

FORRESTER TEI REPORT

We take pride in our privacy practices and are particularly sensitive to making sure our data breaches affect as few customers as possible. We are investing in forensic analysis and cyber analytics. While the costs are increasing today, we think it will help us reduce the cost of data breaches in the future.

SVP // TRANSPORTATION

PONEMON COST OF DATA BREACH REPORT

We’re more confident in the different levels of attacks that it [advanced endpoint security] can detect. It’s able to detect bad behavior and things that are not necessarily file-based. None of our other solutions could do that.

AVP IT SECURITY // FINANCIAL SERVICES

FORRESTER TEI REPORT

INCREASED IT PRODUCTIVITY IS CRITICAL TO BRIDGE THE QUALIFICATION GAP

On-prem security solutions require a large amount of resources to maintain, while cloud-based security enables process automation, increasing the productivity of existing resources.

While this time savings was quantified in the Forrester report, it is also important to note that retention is an added benefit. Productivity of these resources is critical because qualified security analysts are in high demand and hard to hire.

Keeping the qualified resources you have focused on higher tiered activities allows your security team to be more productive in combating threats, but also keeps morale high so you can hold on to these precious resources.

ADVANCED ENDPOINT SECURITY INCREASES EMPLOYEE PRODUCTIVITY

Another benefit Forrester noted that has a widespread impact on business, is the increased performance of employee machines. In fact, Forrester noted that with advanced endpoint security deployed, machines boot in a third of the time they did with legacy AV and experience less lag time when running intensive applications. This time savings adds up across all endpoints.

Additionally, the Forrester study showed a 90% reduction in the need to reimage devices with advanced endpoint security as it stops most threats before they enter the system. This is a big time saver for IT.

EXECUTIVES GAIN VISIBILITY AND CONFIDENCE

With advanced endpoint security, security leaders can produce detailed reports for the C-suite on the status of the company’s protection for specific or potential threats. Security teams can use these tools to conduct thorough investigations and provide visibility for executives on threat risks. This detailed transparency provides executives with confidence in the security of customer data and intellectual property that is critical for doing business in today’s adversarial climate.
Key Steps to Build Your Business Case for Improving Endpoint Security

While this paper has provided much of the evidence needed to convince superiors that investing in advanced endpoint security is good for business, it is often important to personalize this data for your organization. To do this, follow the five steps below to ensure you have data relevant to your business that will prove the value of improving endpoint security and convince your boss to take action.

<table>
<thead>
<tr>
<th>ACTION ITEM</th>
<th>KEY QUESTIONS TO RESOLVE</th>
<th>KEY POINTS FOR YOUR CASE</th>
<th>REFERENCES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STEP 01</strong></td>
<td>Educate your boss on where your security stands against the current threat landscape.</td>
<td>1. Are you in a position where island hopping could be used on you to enter a partner network?</td>
<td>• Quarterly Threat Reports and Research • Verizon Data Breach Investigations Report 2018 • 2018 Cost of a Data Breach Study: Global Overview</td>
</tr>
<tr>
<td></td>
<td>Identify your company’s risk of a material data breach.</td>
<td>2. Can you definitively say whether or not your network has experienced sophisticated attack methods?</td>
<td>• Coalfire Security Maturity Assessment • MITRE ATTACK Framework • The SANS Guide to Evaluating Next-Generation Endpoint Security • NIST Cybersecurity Framework</td>
</tr>
<tr>
<td></td>
<td>Run a maturity assessment to identify gaps in your security stack relative to critical capabilities.</td>
<td>3. Can you validate whether or not threats exist on your network today waiting for the long term attack execution?</td>
<td>• Coalfire Security Maturity Assessment • MITRE ATTACK Framework • The SANS Guide to Evaluating Next-Generation Endpoint Security • NIST Cybersecurity Framework</td>
</tr>
<tr>
<td></td>
<td>Calculate time wasted by security and IT teams using disparate on-premise security tools.</td>
<td>1. The average risk of seeing a material breach in 2019 is almost 30%.</td>
<td>• Coalfire Security Maturity Assessment • MITRE ATTACK Framework • The SANS Guide to Evaluating Next-Generation Endpoint Security • NIST Cybersecurity Framework</td>
</tr>
<tr>
<td></td>
<td>Use your company’s risk and wasted IT team to calculate actual cost savings.</td>
<td>2. Our risk could be higher based on our industry or geographic location.</td>
<td>• Coalfire Security Maturity Assessment • MITRE ATTACK Framework • The SANS Guide to Evaluating Next-Generation Endpoint Security • NIST Cybersecurity Framework</td>
</tr>
</tbody>
</table>

**Key Points for Your Case:**

1. Malicious or criminal attacks are growing and are the cause of over half of data breaches.
2. The majority of these attacks use sophisticated methods that our existing security solutions can’t detect.
3. A data breach of just 10,000 records with our current toolset will cost us $3.86M.

**References:**

- Quarterly Threat Reports and Research
- Verizon Data Breach Investigations Report 2018
- 2018 Cost of a Data Breach Study: Global Overview
- Coalfire Security Maturity Assessment
- MITRE ATTACK Framework
- The SANS Guide to Evaluating Next-Generation Endpoint Security
- NIST Cybersecurity Framework
- Forrester Report: The Total Economic Impact of the CB Predictive Security Cloud

**Summary:**

- Whether above or below average, there are tangible savings to making this investment.
- Employee productivity and morale plus executive confidence are important intangible benefits.
- Attackers aren’t going away. Having appropriate protection is good for customers, partners and investors.