Enterprise Strategy Group by TechTarget

ECONOMIC VALIDATION

The Economic Benefits of DomainTools Internet Intelligence

Earlier Detection and More Comprehensive Domain Intelligence from DomainTools Avoids Organizational Risk and Improves Security Team Efficiency by 79%, While Providing OEM Partners a Return on Investment (ROI) of 1,256%

By Aviv Kaufmann, Practice Director and Principal Economic Validation Analyst
Enterprise Strategy Group

April 2023

Contents

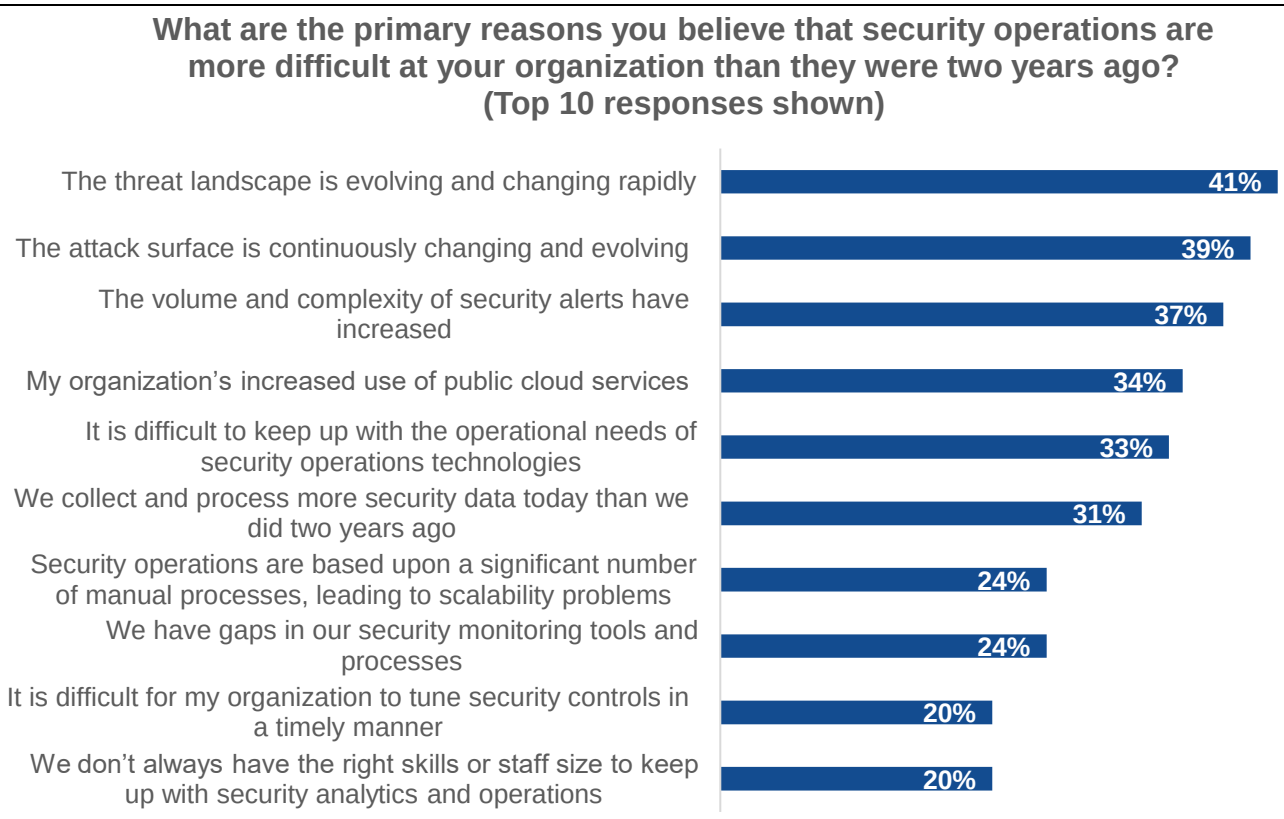
Introduction

This Economic Validation from TechTarget's Enterprise Strategy Group focuses on the quantitative and qualitative benefits that organizations can expect from using DomainTools to help enable their security teams to accelerate threat hunting and intelligence, anti-phishing, counter-fraud, brand protection, and incident response and that security providers can expect from using DomainTools to enrich their applications and/or services.

Challenges

The ability of cybercriminals to quickly spin up infrastructure, share information, and work together in coordinated attacks has resulted in exponential growth in the variety, quantity, and complexity of threats. This makes it much more difficult for security teams to investigate and correlate where attacks originate from or to detect when and where the attackers may pop up next. As shown in Figure 1, Enterprise Strategy Group research identified the top three reasons security operations are more difficult than they were two years ago: the threat landscape is evolving and changing rapidly (cited by 41% of survey respondents), the attack surface is continually changing and evolving (39%), and the volume and complexity of security alerts have increased (37%).[1]

Figure 1. Top 10 Reasons Security Operations Are More Difficult



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Research Brief, *Security Operations Managed Services*, March 2023.

Threat actors often work together to attack from multiple vectors and limit their time spent at a single IP. For security teams, this is like a game of whack-a-mole, as they chase information about IPs, domains, and infrastructure that have disappeared, only to find the attackers showing up and attacking again from another location. With so many emerging threats leveraging attacker-controlled domains across the globe, it is critical to have the ability to investigate and document as much information as possible about the origin of an attack, which other domains attackers are working with or acting against, and any other defining technical or behavioral information that can be used to help detect where attackers may appear next. When hunting for threats, many rely on simple Whois and DNS searches that can provide some basic information about how and when domains were registered, but security teams looking to proactively identify and block access to attackers require more historical context and behavioral correlation to better profile threat actors, phishing sites, and typosquatters, among others, before they become a problem.

The Solution: DomainTools Internet Intelligence

DomainTools provides comprehensive Internet intelligence to security practitioners and advanced security teams. The solutions are used to identify external risks, investigate threats, and proactively protect organizations in a constantly evolving threat landscape. DomainTools constantly monitors the Internet and brings together the most comprehensive and trusted domain, website, and DNS data to deliver context and machine learning-driven risk analytics in near-real time, providing critical tools and services for the following use cases:

- **Threat Intelligence:** Detect relevant indicators earlier in their lifecycle to identify and disrupt incipient attacks.
- **Forensics and Incident Response:** Respond to and triage potential incidents with confidence and speed.
- **Phishing and Fraud Prevention:** Know if and when malicious domains and infrastructure are spoofing your assets before they can cause damage.
- **Threat Hunting:** Discover indicators of compromise (IOCs) and malicious infrastructure that may be targeting your network.
- **Brand Protection:** Monitor lookalike domain names and protect your brand against cybercriminals.
- **Application Enrichment:** Enrich homegrown or third-party security applications with effective Internet intelligence.

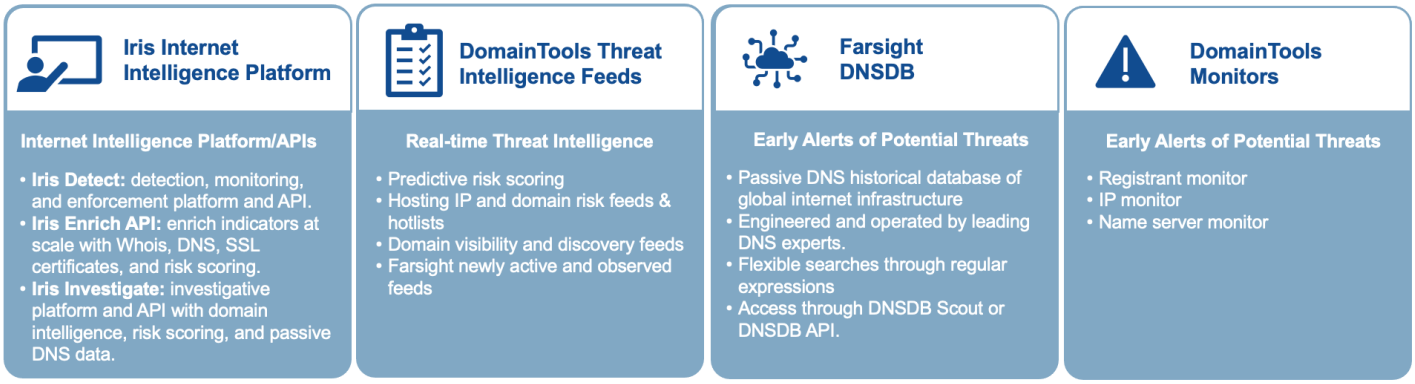
The **Iris Internet Intelligence Platform** is made up of three components, as shown in Figure 2: Iris Detect provides a near real-time internet infrastructure detection, monitoring, and enforcement platform and API; Iris Enrich is a robust API that includes Whois, DNS, SSL certificate, and risk scoring elements to enrich indicators at scale; and Iris Investigate provides a platform and API that supplies and maps domain intelligence, risk scoring, and industry-leading passive DNS data.

DomainTools provides **Threat Intelligence Feeds** that can be integrated into threat intelligence platforms and other tools to provide predictive domain risk scoring, hotlists, newly discovered hostnames and domains, and more.

DomainTools **Monitors** can provide alerts to security teams that signal early warnings of when adversaries are preparing to attack or when known campaigns are evolving.

Farsight DNSDB is a comprehensive passive DNS near real-time and historical database of global internet infrastructure data, that can be accessed and queried by DomainTools customers and integrated into tools through an API to help reduce risk.

Figure 2. DomainTools Internet Intelligence Products and Functions



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group Economic Validation

Enterprise Strategy Group (ESG) completed a quantitative economic analysis of DomainTools services and products. ESG's Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation. ESG conducted in-depth interviews with end users to better understand and quantify how DomainTools has impacted their organizations, particularly in comparison with previously deployed and/or experienced solutions. The customers that ESG spoke with were organizations using DomainTools products to empower and accelerate security teams and functions or were Original Equipment Manufacturers (OEMs) licensing DomainTools services to build more powerful capabilities into their own security products. The qualitative and quantitative findings were used as the basis for two simple economic models comparing the cost and benefits of leveraging DomainTools.

DomainTools Economic Overview

Enterprise Strategy Group found that DomainTools provided security teams and OEM partners with significant savings and benefits in the following categories:

- **Faster Time to Value** – DomainTools was quickly integrated into existing security teams' functions, tools, and processes, as well as successfully licensed by security tool vendors and managed security providers to add domain intelligence to improve their offerings quickly and cost-effectively.
- **Reduced Risk** – DomainTools products provided security teams and OEMs with earlier detection, enhanced coverage, and improved intelligence for potentially harmful infrastructure, helping to significantly lower risk for the organization and its customers.
- **Operational Savings** – By choosing to use and integrate DomainTools products, security teams were able to significantly reduce the amount of time spent on domain-related tasks, and OEMs were able to free up or avoid adding a significant number of resources to better focus on core products and services.

The Benefits of DomainTools for Existing Security Teams and Operations

DomainTools products can be used by security teams to provide and integrate advanced domain intelligence to optimize the effectiveness of various functions within the security organization, including threat intelligence, forensics and incident response, threat hunting, phishing and fraud protection, and brand protection. The teams we

spoke with leveraged the DomainTools Iris Internet Intelligence Platform (Iris Detect, Iris Enrich, and Iris Investigate), Threat Intelligence Feeds, and Monitors. Enterprise Strategy Group validated the savings and benefits that DomainTools was able to provide teams, including the following:

- **Quick to Integrate into Existing Security Workflow** – Customers reported that DomainTools was very simple to integrate into their tools and processes within a few hours and that the simple and intuitive interfaces required very little training or learning before they were able to come up to speed and use the tools effectively. Most reported they were able to realize many of the benefits of using DomainTools within a few days. More customized integration into homegrown tools and scripts took a bit longer, but most reported that any delays were due to internal development scheduling on their end that could easily have been accelerated to a few days if prioritized.

"Out of 1,000 domains determined to be malicious by Iris Detect, 68% did not appear in any other industry-standard blocklist. Of those that were detected elsewhere, Iris Detect and Investigate detected three days earlier on average, with most being detected within a three-hour period."

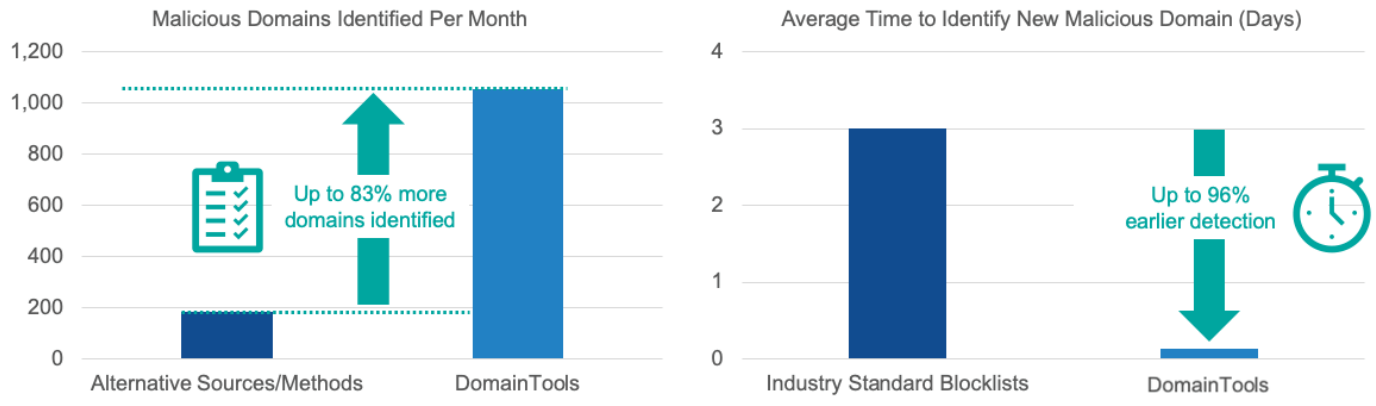
- **More Comprehensive Detection of Malicious Domains** – Threat hunting teams reported that DomainTools was able to dramatically increase the number of potentially malicious domains they were able to identify compared with the feeds and industry-standard blocklists they were using previously. The teams we spoke with were able to share metrics collected before and after using DomainTools and reported that they were able to detect 68% to 96% more malicious domains per month with DomainTools when compared with using industry-standard or open source monitors and blocklists. This enabled teams to take action to block and/or investigate more potentially harmful domains, resulting in reduced risk to the organization.
- **Earlier Detection of Potentially Malicious Domains** – Similarly, threat hunting and intelligence teams reported that DomainTools provided them with significantly earlier detection of potentially malicious domains when compared with the industry-standard blocklists they had relied on previously. Alternative tools and methods they had used rely on reactive detection of malicious activity before identifying and recommending action. DomainTools' comprehensive domain coverage and intelligence was able to quickly detect when known threat actors first set up new domains or coordinated with other known threat actors and then proactively predicted that an attack might be coming before it became an issue. This is not functionality that can be easily achieved by alternative offerings or by a capability built in-house. Teams shared with us that their internal testing had uncovered that industry-standard blocklists generally took three days before malicious domains were identified and added to the list, while these same domains were usually identified and reported in under three hours by DomainTools—and that is in addition to DomainTools identifying far more domains that were not even identified by the industry-standard lists.

"DomainTools gives us the earliest and most updated feed of newly created and updated domain and DNS infrastructure—so the second someone creates a domain, within five minutes, we know about it."

Figure 3 summarizes the improvements DomainTools made in the number of malicious domains identified per month and the reduction in time to identify new malicious domains. These assumptions were used as part of our modeled operational cost savings and risk avoidance, described later in the report.

"Iris Investigate's UI is very well designed and intuitive, so we did not have to have any training before seeing value. If we cannot figure out how to use 80% of a tool without training, honestly we are probably not going to use the tool."

Figure 3. Blended Customer-reported Metrics for DomainTools versus Alternative Methods and Industry-standard Blocklists



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

- **More Visibility and Intelligence into the Domain** – Threat hunting and incident response teams felt that the quality of the domain-related data they were provided by DomainTools was far better and more comprehensive than they could get using alternative tools and manual methods. Other tools and methods (such as alternative commercial offerings or simple Whois searches) simply were not able to provide the same visibility, coverage, and behavioral intelligence. DomainTools has spent over 20 years negotiating the rights to place passive sensors on provider networks to cover 97% of the Internet. Many of the other tools had provided data that was out of date or did not provide enough context to be able to take further steps. This resulted in the manual use of many tools and data sets to correlate data, and, as a result, the work often went undone, increasing risk for the organization. DomainTools reduced the number of data sets that had to be managed by collecting and correlating historical data about actors and interactions between them, providing valuable and comprehensive actor intelligence for investigations that was available and organized before it was needed. A customer stated, *"We did a trial with four different organizations who claimed to provide similar data. DomainTools had better data and faster notifications to the tune of something like 30% better coverage than the other providers that we tested. It was significant and not even a question which we would go with."*
- **Improved Security Insight** – DomainTools provided risk scoring and contextualized insight about malicious domains, which increased confidence in the manual and automated decisions security teams were making. By being able to identify and understand malicious actors better, as well as their behavior over time—with a credible and quantified risk score associated with each domain and host—organizations were able to combine powerful domain-related intelligence with other tools and processes to better stay on top of a continuously changing threat landscape.

> **"The statistics that we get are very useful. We were able to see that over 50% of the malicious domains were being generated from a single region, and which ISPs and registrars they were originating from. This would be near impossible to achieve at this scale without DomainTools."**

- **Improved Security Posture and Fewer Attacks** – With the information and tools provided by DomainTools, security teams were able to identify potential threat actors and campaigns earlier and investigate and remediate threats faster. Teams reported that they felt DomainTools products contributed to an overall more effective security posture around avoiding brand monitoring, phishing, malware, and spam attacks. They were able to proactively identify zero-day threats and help close the window of opportunity for potentially malicious

attacks more quickly. The earlier detection provided by DomainTools gave them a better opportunity to investigate, block, and disrupt attacks, resulting in fewer successful incidents that would later require a reactive response.

- **Improved Productivity for Security Teams** – Customers of DomainTools' products reported that they were able to free up time versus having to perform manual tasks, such as performing Whois searches and DNS lookups, managing SSL certificates, and correlating results. Some reported that it saved them 1.5 to 2 hours per day, enabling them to be more productive in other areas and cover more cases and alerts. Risk scoring profiles for domains helped them to identify the top priorities, automate decision-making intelligence, and better categorize threats. Enrichment of indicators allowed them to be more efficient in investigations and provide faster responses by being proactive and having intelligence populated before it was needed.
- **Improved Security Workflows** – Similarly, by using the Iris Internet Intelligence Platform and integrating DomainTools products into existing security tools and processes, organizations were able to simplify and accelerate security workflows, reducing the number of interactions required and improving collaboration across teams. Customers reported that they were able to triage and perform investigations and then export the investigation to other functions to further transform and enrich the intelligence for optimal use by incident response teams. This eliminated the inefficient reliance on manual steps and email interactions to pass information back and forth.

"We achieve a higher level of quality with DomainTools and free up time to investigate deeper, collaborate, and make time to support other processes as well. This makes our security team as a whole much more effective."

Enterprise Strategy Group Analysis: Security Team Scenario

Enterprise Strategy Group (ESG) leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and the results of customer interviews to create good-faith models and scenarios that compare the costs and benefits of leveraging DomainTools versus alternative tools and methods. ESG's interviews with customers who have recently made the transition, combined with ESG's experience and expertise in economic modeling and technical validation of security technologies, helped to form the basis for all modeled scenarios shown in this report.

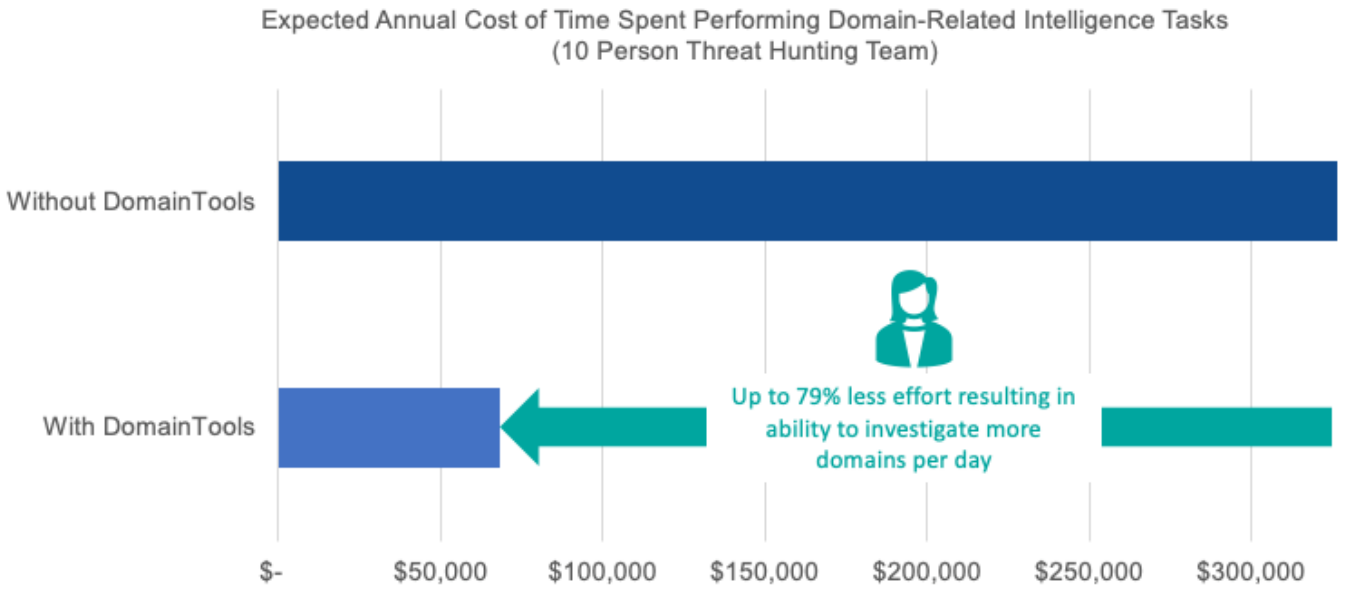
For our first scenario, ESG modeled the expected costs and benefits of leveraging the DomainTools Iris Internet Intelligence Platform rather than relying on industry-standard threat intelligence feeds and blocklists, along with open source tools, to obtain domain-related information. We assumed that a large organization with a potential attack surface spanning 35,000 subdomains relied on a team of 40 analysts to provide threat hunting, threat intelligence, and incident response. Ten analysts were responsible for threat hunting activities to protect the organization and its customers from potential phishing, pharming, spam, and typo-squatting attempts. We conservatively assumed that the team currently spent roughly 20% of their time on domain-related intelligence tasks (the equivalent of two full-time analysts, or 3,840 hours per year). By using DomainTools, customers reported that they saved between 1.3 to 2 hours per day by not having to perform manual functions. As shown in Figure 4, with two analysts each saving a conservative 1.3 hours per day, they will save 3,040 hours per year, reducing the time and cost to perform the equivalent number of domain-related intelligence tasks by 79% and avoiding roughly $259K in operational costs. This avoided cost can perhaps better be thought of as improved productivity, as, given the same amount of time to investigate domains, those using DomainTools can work on 79% more tasks, resulting in more value and reducing risk further for the organization.

Why This Matters

Security teams struggle to keep up with infrastructure, domains, and DNS services quickly deployed and used by threat actors over an expanding attack surface before disappearing.

Enterprise Strategy Group validated that DomainTools can help security teams identify and make decisions to block potentially harmful assets used by cybercriminals earlier and more effectively than alternative methods in use today. DomainTools helped security teams save time and maximize coverage to help reduce risk to the organization.

Figure 4. ESG's Modeled Annual Savings for a 10-person Threat Hunting Team Using DomainTools

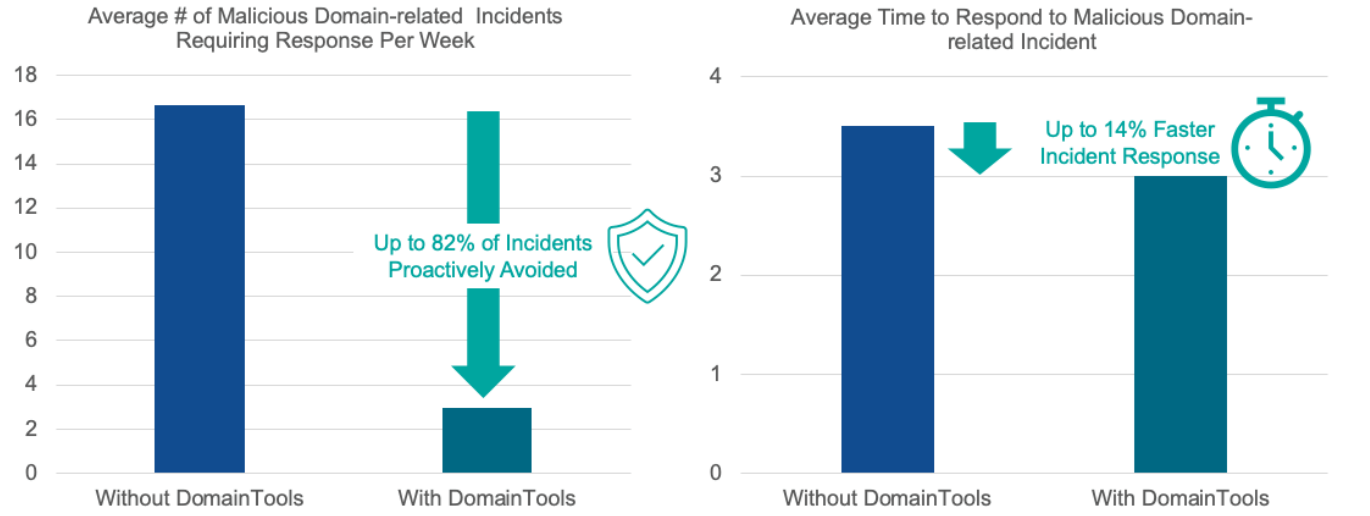


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Next, ESG modeled the expected savings and benefits an organization might realize around domain-related incident response. Using blended results from our interviews with large organizations, we assumed a total of 1,086

new potentially identifiable malicious hosts and domains originated per month. We then assumed that DomainTools could identify 97% of the potentially malicious domains in under three hours, while industry-standard blocklists would take three days to identify domains and only report on about 17% of the new domains. Then, using ESG's proprietary model that ranks risk of incident versus time to identify threats before they develop into incidents (under one hour, under a day, under three days, or unidentified), we concluded that the organization could expect to respond to about 17 incidents per day without DomainTools and only three incidents with DomainTools. We also assumed that DomainTools platforms could reduce the time to respond per incident from 3.5 hours to 3 hours. Modeling out the time spent and associated costs, we concluded that DomainTools could eliminate 82% of the incidents requiring response and reduce time to respond by at least 14%, resulting in annual savings of $219K, as summarized in Figure 5.

Figure 5. ESG's Modeled Improvement to Incident Response with DomainTools



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Next, ESG leveraged the risk-adjusted expected annual cost to an organization due to phishing-related activity, as measured and reported by the Ponemon Institute, of $14M. This cost takes into consideration all of the risk-adjusted impacts of malware, ransomware, and business email compromises, as well as the associated productivity loss, costs to contain the incidents, and revenue loss. While the true cost would be in the hundreds of millions of dollars for such an event, the $14M number represents the annual "expected cost" weighted against the probability of events happening. The report mentions that organizations can reduce this expected cost by up to 53% with proper training. We assumed this was the case and used $7.8M as our baseline risk number. We then assumed an annual probability of 3% for a successful attack on the baseline organization and a 0.5% probability of a successful attack for DomainTools, with the lowered probability based on the 82% improvement in number of avoided incidents. This resulted in a conservative annual expected avoided risk of $365K.

Taking all of these results into consideration, ESG models predict that DomainTools Iris Internet Intelligence Platform could save a large organization $844K per year in improved operational efficiencies, avoided incidents, and reduced risk to the organization. As shown in Figure 6, this results in an expected annual return on investment (ROI) of 740%.

Figure 6. Expected Annual Return on Investment for DomainTools

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Benefits of DomainTools for OEM and Service Providers

DomainTools Intelligence Feeds, Monitors, APIs, and FarsightDNSDB query capabilities can be licensed and integrated into custom in-house tools for security teams, as well as into products and services offered by OEM partners. By integrating these technologies into their own product, their security teams and customers can take advantage of many of the same domain-related intelligence savings and benefits that are delivered by DomainTools own products. Enterprise Strategy Group interviewed several OEM partners to validate the experiences, savings, and benefits that they had seen since building DomainTools technologies into their own products and services. These OEM partners reported the following benefits:

- **Faster Time to Advanced Product Capabilities** – The OEMs we spoke with were able to integrate comprehensive domain threat intelligence into their products on only a few short sprints (about four weeks) versus the no shorter than 10-12 months of development and testing time they predicted it would take to only start to build similar, but nowhere near equivalent, capabilities with their own development resources. This allowed them to release product features and functionality up to 11 months earlier.
- **Significantly Fewer Resources Required** – By integrating DomainTools rather than building capabilities in-house, OEMs freed up a significant amount of development, test, and support resources. Some estimated that it would take a full-time team of ten developers to first build and then maintain and support the capabilities going forward, versus only two developers and a few sprints for initial integration, and then only a few hours per year to maintain the integration. Most of the support issues related to the integration could often be passed to DomainTools support and developers to resolve quickly and effectively.

> **"If we were going to build similar capabilities, we would have to develop an awful lot of services from scratch. The number of services you would have to build is very large and complex, and the end product would not be nearly as complete as what you can get by integrating DomainTools."**

- **Improved Product Quality and Complementary Capabilities –** As described in the earlier sections of this report, it would be nearly impossible for OEMs to create the same capabilities and match the coverage and effectiveness provided through an integration of DomainTools technologies. OEMs were able to integrate DomainTools to improve their product and service abilities for earlier detection of typosquatters, threat intelligence reporting, improved domain intelligence for making infrastructure-related decisions, and automated enrichment and attribution for investigations. This would not only require substantial development efforts, but also a near impossible number of legal contracts and custom agreements to place sensors across 97% of the Internet. By combining product capabilities and potential attack surface coverage, OEMs were able to produce a substantially improved and more effective product.

"As an OEM, DomainTools provides us with the data to make our security products more effective and intelligent and the tools used by our services to provide quicker and more actionable insight to our customers."

- **Improved Market Share and Revenue –** By releasing product capabilities up to 11 months earlier and providing a product with improved quality and capabilities, OEMs were able to start to benefit from increased revenue streams and gain market share from competing products. OEMs could choose to offer advanced domain services as an add-on benefit, generating new streams of revenue, or not charge extra and instead benefit from increased market share gained by offering a superior service and value compared to alternatives. One customer stated, *"Customer satisfaction with our product since we have released the capabilities has gone significantly up. It has helped us to close more deals and has helped us to identify true positive threats for customers earlier and those that we would not have otherwise seen."*

"I can tell you that we have already won more deals based on having the features we built with DomainTools that support more than the cost of our contract, and we've been out less than a year with those features."

- **Improved Managed Security Services** – OEM partners also revealed that, in addition to building the capabilities into their own products, they also used the Iris platform and other tools to improve the effectiveness of their threat hunting and incident response managed services as well. By doing so, they enjoyed all of the operational benefits described in the security teams scenario in this report, and they were able to pass on many of the benefits of earlier detection and faster response to help lower risk for their clients. *"The DomainTools team is fantastic about connecting with my engineers, connecting with my threat intelligence researchers, doing training, providing support, and making sure we're really maximizing the value of the product."*

"DomainTools gives us confidence in our decisions on what can be shut down, but it also helps us perform due diligence to make sure that what we will shut down is not going to cause problems for our customers."

Enterprise Strategy Group Analysis: OEM Scenario

To illustrate the potential ROI of OEMing and integrating DomainTools technologies into an existing product, we leveraged the blended assumptions reported to us in our interviews on the time and effort expected to license and integrate DomainTools versus building these capabilities in-house. Our proprietary model assumed that DomainTools would require an annual contract and could be integrated into a product in only four weeks with a team of two full-time developers. Building capabilities in-house would require a team of ten developers over 48 weeks (ten months) to start to build this functionality, leveraging industry-standard domain information and a few negotiated agreements with provider networks willing to allow sensors to be placed. It should be noted that the result would not be as effective as DomainTools' integration, which took over 20 years to build, and a newly built tool would certainly have reduced capabilities in comparison.

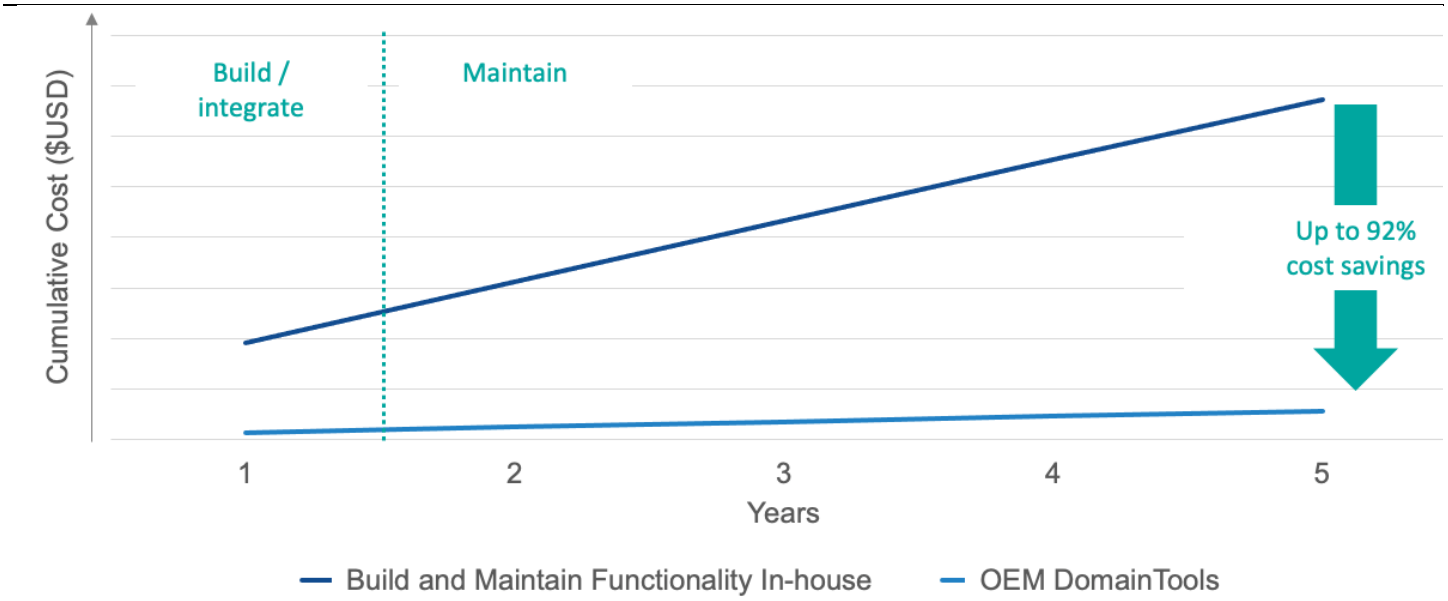
For ongoing support, we assumed that the DomainTools OEM would require the equivalent of one developer cumulatively spending roughly two weeks (80 developer hours) per year to manage support, updates, and changes. In contrast, an in-house solution would require a team of eight full-time developers (15,360 developer hours) to perform maintenance and support, manage contracts and zone files, maintain a discovery and historical tracking system, carry out risk scoring, and execute many other functions to keep things running while continuing to grow coverage. Figure 7 compares the expected costs over a five-year period resulting in an annual average cost savings of 92% to license and integrate DomainTools rather than attempt to build similar functionality in-house.

Why This Matters

Just like security teams, security products and services looking to better protect organizations require the best domain intelligence possible to operate effectively.

Enterprise Strategy Group validated that OEM partners of DomainTools were able to integrate top tier domain intelligence into their products and services far quicker and more cost effectively than if they had tried to build the functionality by themselves, resulting in a higher quality product and better protected customers.

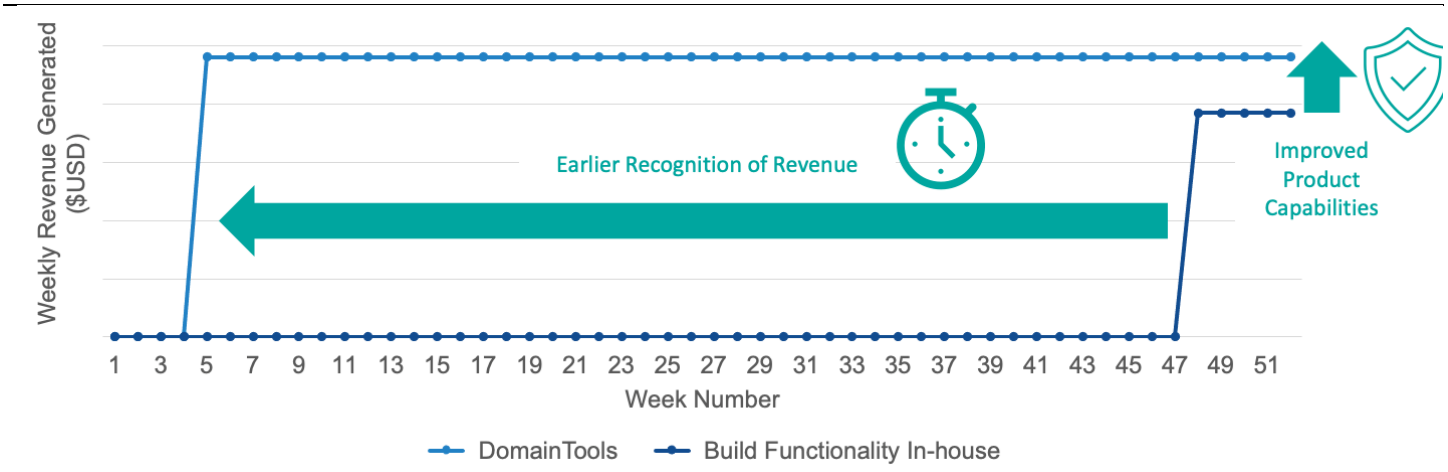
Figure 7. Cumulative Expected Cost to Build Effective Domain Enrichment and Risk Scoring Using DomainTools versus In-house Functionality



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The operational cost savings alone makes a very compelling case, but it gets better. By having a product that is live and ready far quicker, organizations can start to generate revenue, gain competitive differentiation and market share, and avoid churn with existing customers months earlier. And because the product built with DomainTools offers significantly more comprehensive capabilities than could realistically be achieved in-house in such a short time, the expected revenue impact per month could realistically be much higher, as well. Figure 8 illustrates this example. Using very conservative assumptions, Enterprise Strategy Group's estimates predicted that DomainTools could provide an organization enhancing a $50M product offering (assuming a very small 0.8%-1% revenue increase) with at least $423K in the first year (mainly from earlier realization of revenue streams) and $100K for each additional year (due to improved product capabilities).

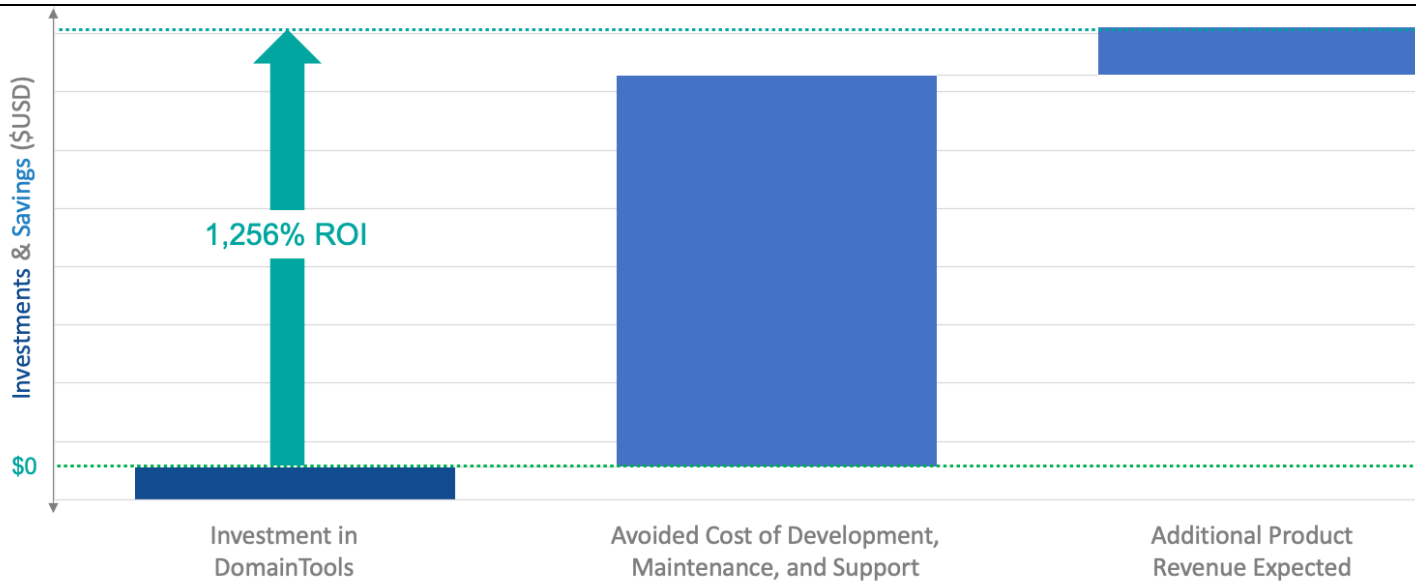
Figure 8. Expected Weekly Revenue Generated as a Result of Adding Effective Domain Enrichment and Risk Scoring Using DomainTools versus In-house Functionality



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Using our modeled results and licensing cost estimates provided by DomainTools, Enterprise Strategy Group calculated an ROI over the first year of 1,710% (or a 17x return in the first year). Once the product development work is complete and the product has been released, the expected ongoing ROI levels off to 1,143% (11x return) per each additional year as the product is maintained. As shown in Figure 9, if measured over a five-year period, the organization could expect an impressive ROI of 1,256% (12.5x return).

Figure 9. Expected 5-year ROI for a DomainTools OEM



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Issues to Consider

Enterprise Strategy Group (ESG)'s models are built in good faith upon conservative, credible, and validated assumptions; however, no single modeled scenario will ever represent every potential environment. DomainTools has a number of offerings that can be used across many functions and integrated into many tools and services. The benefits received by an organization depend on the size of the organization, the nature of the business, and the current capabilities of the security team, product, or service, along with many more variables. ESG recommends that you perform your own analysis of available products and consult with your DomainTools representative to understand and discuss the differences between the solutions through your own proof-of-concept testing.

Conclusion

Timely and comprehensive domain and DNS-related threat intelligence is critical to protecting any organization or application, but security teams have limited human resources and budgets. This can result in missed information and ineffective protection. Security teams must strive to be proactive rather than reactive. Threat intelligence generated after a malicious act is delivered too late and cannot be addressed in a timely manner. Further, contextualizing investigations with domain information generated solely on the current state is not useful. Decisions made based on limited visibility of the infrastructure or domain intelligence generated without proper historical and threat actor behavioral context results in reduced quality of insight. All of this results in opportunities and advantages for the attackers.

One customer summed it up very well: *"DomainTools has done a fantastic job of closing the gap on discovery, and I really think they have a core advantage because of this fact. They've been in the business for 20 years. I know what it takes on the back end to get that data, and it is incredibly hard. They are doing a fantastic job getting information in the areas where criminals tend to congregate and where the threats tend to be located. And if you're just pulling zone files, that is what you will miss. It's not the threats you find, or that everybody finds, that are the problem. It's the ones that are hard to find, that sneak under the radar, that are the most critical and that provide the most value. And that's where we really see value with DomainTools."*

Security teams not only see significant operational savings (up to 79%) and effectiveness (up to 83% more domains identified and up to 96% faster detection) with DomainTools, resulting in far lower risk to the organization; one security team mentioned, *"Our investment in DomainTools could save us 100 to 1,000 times what we pay if just one of these attacks were successful."* OEMs describe DomainTools as a partner and a force multiplier to their products, even when their products provide similar benefits to end-users. By combining their coverage and offering a "better together product" that covers an even greater attack surface, everyone but the threat actors win. Our models show that choosing to OEM DomainTools makes great business sense and results in significantly quicker capabilities and a very large ROI (1,245%).

If your organization is looking to provide effective domain intelligence for your security operations, products, or services, Enterprise Strategy Group strongly recommends that you consider DomainTools.

About Enterprise Strategy Group
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

contact@esg-global.com
www.esg-global.com