TANIUM

WHITEPAPER

Bewältigung der größten je dagewesenen Angriffsfläche mit Converged Endpoint Management (XEM)

Zusammenfassung

Ransomware-Angriffe sind eine der am schnellsten wachsenden Cyber-Bedrohungen in der jüngsten Geschichte. Die Anzahl der Angriffe stieg im 3. Quartal 2021 um über 140 %, obwohl Unternehmen letztes Jahr über 160 Milliarden USD für Cybersecurity ausgegeben haben.

Haben Sie sich jemals gefragt, warum dieses Problem mit hoher Priorität mehr Geld und Aufmerksamkeit als je zuvor erhält, und es trotzdem immer schlimmer wird?

Das liegt daran, dass der Sicherheitsansatz der Branche fehlerhaft ist.

Die Lösungen von IT-Sicherheits- und Managementanbietern leisten jeweils nur einen geringen Beitrag zum Schutz unserer Umgebung. Und die Situation wird noch dadurch verschärft, dass diese verschiedenen Tools oft in Silos in verschiedenen Organisationen eingesetzt werden.

So sind CIOs und CISOs zur Anschaffung und Integration verschiedener Lösungen gezwungen und müssen Entscheidungen anhand veralteter, falscher und unvollständiger Daten treffen.

Obendrein fehlt es diesen Tools an Echtzeit-Transparenz. Tatsächlich fehlen in 94 % der Unternehmen bei ihren Tools möglicherweise bis zu 20 % der Endpunkte, die einen Schutz erfordern. Point Solutions schaffen Lücken, die Hacker ausnutzen können, und nur zur Komplexität einer ständig wachsenden Angriffsfläche beitragen.

Halten Sie einen Moment inne. Wann haben Sie sich das letzte Mal diese Fragen gestellt?

- Wie viele Endpunkte haben wir?
- Welche Anwendungen laufen auf ihnen?
- Welche Benutzer haben unnötigerweise Administrator-Berechtigungen?

Mussten Sie zur Beantwortung dieser Fragen mehrere Point Solutions nutzen und dann die Daten jeder Lösung zentralisieren, normalisieren und analysieren?

Es ist an der Zeit, diesen Zyklus mit einem völlig anderen Ansatz zu beenden: der Bereitstellung einer „Converged Endpointmanagement Plattform."

Eine einzige Plattform, die Visibilität und Behebung bereitstellt.

Eine zentrale Plattform, die Echtzeitdaten liefert und Aktionen in Echtzeit umsetzt.

Diese Plattform verwaltet und schützt jede Art von Endpunkt, vom Laptop über Cloud-Container bis hin zu Sensoren und Internet of Things (IoT), sodass Teams zusammenarbeiten können, indem sie Daten über IT-Operations, Security und Risk- und Compliance-Management hinweg zusammenführen. Wenn Sie diesen Plattformansatz verfolgen, statt verschiedene Point Solutions zusammenzustellen, werden Sie sehen, dass es möglich ist, mit jedem Endpunkt in Sekundenschnelle zu interagieren, unabhängig von Netzwerkskalierung und Komplexität.

Unternehmen verfügen jetzt über eine „Converged Endpointmanagement Plattform", der sie sowohl vertrauen als auch weiterhin vergrößern und erweitern können. Sie können das angesammelte Chaos aus alten Point Solutions leicht und systematisch entfernen und es durch eine einzige Plattform ersetzen.

Die Entwicklung von Technologie und Gesellschaft

Wir befinden uns in einer dynamischen Zeit, in der wir Veränderungen sowohl in der Technologie als auch in der Gesellschaft erleben, die sich auf unsere Arbeitsweise und unser Leben auswirken. Jede Organisation steht vor diesen drei großen Veränderungen:

Digitale Transformation

Die digitale Transformation verändert die Art und Weise, wie Unternehmen in jeder Branche tätig sind und ihren Kunden Mehrwert bieten. Was früher zentral von Sicherheitsperimetern gesteuert wurde, hat sich zu einem ausgedehnten Netz aus Softwarediensten, Cloud-Infrastrukturen und dezentralen Anwendungsdiensten entwickelt.

Laut dem Forschungsunternehmen Futurum geben Unternehmen jetzt jährlich 700 Milliarden US-Dollar für digitale Transformationsprojekte aus. Die Studie zeigt auch, dass das typische Unternehmen über mehr als 200 aktiv verwendete Anwendungen verfügt und 60 % dieser Anwendungen alle zwei Jahre umgestellt werden. Dieses Tempo der digitalen Transformation stellt eine große Herausforderung für die Cybersecurity dar.

Arbeiten von überall.

Der Anstieg der Remote-Arbeit durch die Pandemie hat zu einem sich ständig ändernden dynamischen Perimeter geführt.

Vor der Pandemie verfolgten die meisten Unternehmen einen mit Mauer und Burggraben vergleichbaren Ansatz für die Cybersecurity. Unternehmens-Firewalls schützten Unternehmensnetzwerke und gewährleisteten die Sicherheit von lokalen Geräten, Systemen und Daten.

Dieser Ansatz funktioniert heute nicht mehr so gut. Viele IT-Ressourcen arbeiten jetzt außerhalb des Grabens – oder der Firewall – und sind anfällig für Cyberbedrohungen aller Art.

Wenn Unternehmen nicht in der Lage sind, die Sicherheit auf diesen Geräten zu verwalten, unabhängig davon, wo sie sich befinden, bieten sie eine große Angriffsfläche und öffnen sich einem massiven Risiko.

Endpunkt-Explosion

Schließlich führt die Kombination aus digitaler Transformation und Arbeit von überall aus zu einer Explosion bei Endpunktgeräten, die die Grenze um mobile Geräte, IoT, Cloud-Container und Sensoren erweitert – allesamt potenzielle Ziele für Angreifer.

Unterdessen stellen immer ausgeklügeltere Angriffe wie Phishing, Kompromittierung geschäftlicher E-Mails, Ransomware und andere eine weitaus schwierigere Herausforderung für das Endgerätemanagement dar als je zuvor.

Als Reaktion auf diesen Druck erwerben IT-Teams immer mehr Tools, und diese Anschaffungen werden allzu oft vom Team isoliert. Eine Studie von Tanium zur Visibility Gap im Jahr 2020 ergab, dass das durchschnittliche Unternehmen ca. 43 Tools für IT-Betrieb und -Sicherheit verwendet, obwohl das je nach Unternehmensgröße stark variiert.

Aber trotz weiterer Tools und wachsender Sicherheitsbudgets verbessern sich die Schwachstellen nicht. Es wird tatsächlich schlimmer. Organisationen geben Milliarden für Cybersecurity aus. In der Zwischenzeit werden 20 % der Endpunkte weder entdeckt noch geschützt, und ein Ransomware-Angriff findet immer noch alle 11 Sekunden statt.

Es ist heute schwieriger denn je für CIOs und CISOs, den Betrieb zu gewährleisten und zu schützen.

Mehr Komplexität, mehr Herausforderungen

Unternehmen sehen sich außergewöhnlichen Umständen gegenüber. Es ist einfach, Endpunkte zu verwalten, wenn die Angriffsfläche nicht wächst, oder die digitale Transformation anzuleiten, wenn sie nicht über Nacht stattfinden muss.

Wie ermöglichen Sie also neue und aufkommende Technologien und die digitale Transformation in diesen schwierigen Zeiten?

1. Modernisieren Sie Ihre alten Plattformen, Ansätze und Umgebungen.
2. Verwalten Sie laufende Compliance- und regulatorische Anforderungen.
3. Besseres Management von Sicherheitsbedrohungen und wachsender Angriffsfläche.

Lassen Sie sich nicht täuschen: Während wir immer vernetzter werden, werden die Bedrohungen immer realer. Mit einer größeren Angriffsfläche werden die Bedrohungen immer komplexer und schwieriger zu verteidigen. Und die Angreifer, die oft staatlich gesponsert werden, nutzen dieselben neuen Technologien, um einen hochentwickelten Krieg gegen uns zu führen.

Wir brauchen eine Konvergenz.

Warum jedes Unternehmen XEM benötigt

Konvergente Lösungen vereinen Tools und Daten in einer einheitlichen Lösung. Eine konvergente Lösung ist ein System, das Konvergenz ermöglicht: Es dient als Rückgrat für alle wichtigen Interaktionen zwischen Daten, Tools und Teams. Es befindet sich an der Schnittstelle zwischen IT Operations-, Security-, Risk- und Compliance-Management. Konvergente Lösungen sprechen eine Vielzahl von Nutzern an und ermöglichen es IT-Führungskräften und Mitarbeitern, zusammenzuarbeiten.

Veränderungen und Wachstum müssen gemanagt werden

Unternehmen benötigen eine Lösung, die Endpunktexplosion, Toolverbreitung und IT-Modernisierung für jeden Endpunkt, jeden Workflow und jedes Team löst.

Angesichts der Vielzahl von Änderungen, die sich auf die IT auswirken, ist es wichtig, dass Unternehmen Lösungen priorisieren, die Transparenz über alle ihre Endpunkte hinweg, die Kontrolle über diese Endpunkte und das Vertrauen in die Qualität der generierten Daten bieten. Es ist von größter Bedeutung, dass Unternehmen die Verbreitung von Tools und die Ermüdung bekämpfen, die nur die Risikoexposition eines Unternehmens erhöhen und die Produktivität der Mitarbeiter durch die Konsolidierung von Tools senken. Silos innerhalb von Unternehmen können mit gängigen Tools entfernt werden, die IT-Operations, Risk und Compliance sowie Security zu einer konvergenten Plattform kombinieren.

Eine konvergente Plattform, wie die beschriebene, muss drei Dinge abdecken:

- Jeden Endpunkt. Die Sichtbarkeit über die gesamte Bandbreite von Endpunkten über eine einzige Oberfläche ist ein Muss; ob Laptop, Desktop, Mobil, Container, Sensor – alle Arten von Endpunkten müssen bekannt, verwaltet und geschützt sein.
- Jeden Workflow. Das Potenzial, Maßnahmen zu ergreifen und jeden Workflow zu erstellen, den ein Unternehmen benötigt, muss über eine Plattform aktiviert werden: Jedes Modul (ob IT-Operations, Security oder Risk & Compliance) ist lediglich ein Workflow, der auf den gleichen zugrunde liegenden Plattformfunktionen basiert.
- Jedes Team. Die Ausrichtung zwischen Teams auf eine „Single Source of Truth“, die gleichen Daten und die gleichen gemeinsamen Tools ist ein Grundbedarf, um Silos abzubauen.

Konvergente Plattformen meistern die Herausforderung „Technologie-Prozess-Menschen“

Eine einheitliche Plattform, die eine schnellere Entscheidungsfindung, High-Fidelity-Daten und mehrere Funktionen an einem Ort ermöglicht, ersetzt mühsame manuelle Prozesse. Durch die Kombination der Reichweite von IT-Betrieb, Security sowie Risk & Compliance an einem Standort wird erreicht, was mehrere veraltete Point Solutions nicht können. Teams können sich auf das Wesentliche konzentrieren, ihre Arbeit funktionsübergreifend, produktiv und sicher erledigen und die effektivste Reaktion auf ein Umfeld bieten, in dem Angreifer aggressiver als je zuvor und Kunden anspruchsvoller denn je sind. Wie ermöglichen Sie also neue und aufkommende Technologien und die digitale Transformation in diesen schwierigen Zeiten?

Ergebnisse von XEM

Dieser konvergente Ansatz befähigt Kunden in vier kritischen Bereichen:

Visibilität: Mit vollständiger Visibilität können Unternehmen Risiken identifizieren, indem sie die Endpunktumgebung innerhalb von Minuten scannen. Dies ist wichtig, wenn Sie an den sich ständig ändernden Perimeter denken, bei dem Geräte kommen und gehen, oder wenn Sie IoT-Geräte oder Sensoren hinzufügen.

Ausrichtung: Aus einer Ausrichtungsperspektive können Sie eine gemeinsame Sprache zwischen Betriebs-, Sicherheits- und Risikoteams finden – alles mit einem gemeinsamen Datensatz.

Reaktionsfähigkeit: Durch Reaktionsschnelligkeit können Sie Schwachstellen beheben und Compliance-Probleme mit einem Klick und einer Konsole in Sekundenschnelle lösen.

Kontrolle: Sie können den Perimeter von Operations, Security und Compliance dorthin verschieben, wo das Netzwerk wirklich beginnt und endet – an die Edge.

XEM-Anwendungsfall: Log4j

Es gibt keinen besseren Anwendungsfall von XEM als die branchenweit kritischste Schwachstelle, Log4j. Mit einer konvergenten Plattform konnten Kunden detaillierte und vollständige Ermittlungen in Echtzeit, eingehende Bewertungen, Priorisierung und plattformübergreifende Betriebssystem-unabhängige Behebung durchführen.

Eine XEM-Lösung kann Indikatoren für Schwachstellen finden, Anzeichen von Ausbeutung erkennen, beheben und die Umgebung schützen und laufende Risiken melden. All diese zusammenarbeitenden Komponenten unterscheiden die XEM-Plattform von allen anderen Produkten auf dem Markt.

Definieren von Fähigkeiten

Konvergente Plattformen lösen das Technologieproblem, sodass sich Unternehmen auf das organisatorische Problem konzentrieren können.

Technische Lösungen sollten die Grenzen der Technologie überschreiten. Sie müssen eine Geschäftslösung ermöglichen. Durch eine bessere Kommunikation unter Teams und durch Visibilität in ihre Assets können Teams schneller fundierte Entscheidungen treffen, weil sie bessere Kontrolle über die Assets und die damit zusammenhängenden Daten haben. In der Vergangenheit war die Verantwortlichkeit aufgrund von beschädigten Tools und isolierten Teams begrenzt – aber dies ist nicht mehr der Fall mit dem Aufkommen konvergierter Tools. Vorbei sind die Zeiten unzuverlässiger Tools und unterbrochener Prozesse, die zu unvollständigen Ergebnissen führen.

Konvergente Plattformen stellen die Produktmentalität der alten Schule auf den Kopf

Anstatt toolorientiert zu sein, sind konvergente Plattformen geräteorientiert. Anstatt Tools auf den Endpunkt anzuwenden, berücksichtigen konvergente Plattformen alles, was der Endpunkt benötigt, und machen den Endpunkt zum Fokus. Konvergente Plattformen bieten alles, was für die Reise oder den Lebenszyklus eines Geräts erforderlich ist. Produktteams, die konvergente Plattformen entwickeln, werden eine ganzheitliche Denkweise annehmen, die Roadmaps skizziert, die die verschiedenen Bedürfnisse des Endpunkts abdecken – von einem operativen zu einem Compliance- bis hin zu einem Schutzstandpunkt.

Konvergente Plattformen vereinen Tools und Daten in einer einheitlichen Lösung.

Mehrere Kernfunktionen umfassen konvergente Plattformen, die in einer einzigen Oberfläche untergebracht sind – ein Dashboard, um alles zu sehen, zu steuern und allem zu vertrauen, was am Endpunkt passiert. Die Visibilität aller Daten von allen Endpunkten an einer Stelle:

1. **Risk- & Compliance-Management:** Überwachen von Datei- und Registry-Änderungen; Einhaltung von datenschutzrechtlichen Bestimmungen und Praktiken. Durchsuchen des Netzwerks nach nicht verwalteten Assets; Finden von Compliance-Lücken; -Bewerten des Computers anhand von Branchen-Benchmarks.

2. **Client-Management:** Führen Sie Patches konsistent und schnell durch. Sorgen Sie mit automatisiertem Patching und minimalen Ausfallzeiten dafür, dass alle Systeme laufen und auf dem neuesten Stand sind; vereinfachen, zentralisieren und erzwingen Sie kritische Konfigurationen.

3. **Threat Hunting:** Ausgabe von Warnungen zu verdächtigem Verhalten und Wiederherstellung von Endpunkten in den stationären Zustand. Identifizieren Sie risikoreiche Konten und Systeme, suchen und beheben Sie Schwachstellen in großem Maßstab und führen Sie auf Endpunkten eine automatische Behebung durch priorisierte Aktionen durch.

4. **Asset-Discovery und -Inventory:** Führen Sie eine vollständige Bestandsaufnahme der Hardware- und Software-Assets durch. Identifizieren aller Rechner im Netzwerk einschließlich der aktuellen Software und deren Verwendung.

5. **Überwachung sensibler Daten:** Verfolgen und Verwalten sensibler Daten, damit Angreifer dies nicht können. Schnell nach sensiblen Daten suchen und ihren Speicherort identifizieren, um Maßnahmen zu ergreifen. Unberechtigte Änderungen in Dateipfaden finden, das System auf Datenexposition und potenzielle Risiken überprüfen und Dateisysteme indizieren.

6. **Servicemanagement:** Hilft den IT-Teams bei der Unterstützung von Mitarbeitern und der Behebung von Helpdesk-Tickets. Straffen der Arbeitsabläufe des Helpdesks mithilfe von genauen Echtzeitdaten.

Konvergente Plattformen sprechen eine Vielzahl von Benutzern an

CIOs entscheiden sich für konvergente Plattformen, um sicherzustellen, dass ihre Endpunkte innerhalb weniger Stunden auf die neuesten Schwachstellen gepatcht und entsprechend konfiguriert werden. CISOs entscheiden sich für konvergente Plattformen, die als letzte Verteidigungslinie für die Reaktion auf Vorfälle dienen. Infrastrukturteams nutzen konvergente Plattformen, um Cloudmigrationen innerhalb von Wochen anstatt Monaten oder Jahren durchzuführen. Beschaffungsteams verwenden konvergente Plattformen, um zu validieren, dass sie nicht für mehr Software bezahlen als sie verwenden. Auditoren nutzen konvergente Plattformen, um zu bewerten, wie gut Unternehmen die Vielzahl von regulatorischen und Compliance-Rahmenwerken einhalten. Datentreuhänder verwenden konvergente Plattformen, um sensible Daten in großem Maßstab zu finden und zu entfernen.

Konvergente Plattformen ermöglichen natürlich IT-Führungskräften und -Mitarbeitern – über eine Reihe von Funktionen hinweg –, alle ihre Assets zu verwalten und zu sichern.

Blick in die Zukunft

Trends, die die heutige IT-Welt prägen, werden sich nur noch beschleunigen

Trends bei der Remote-Arbeit bleiben erhalten. Die Notwendigkeit, alle Arten von Endpunkten (innerhalb und außerhalb des Netzwerks) zu verwalten und zu sichern, verschwindet nicht. Laut einer Umfrage von Gartner werden 48 % der Mitarbeiter zumindest teilweise nach Ende der Pandemie aus der Ferne arbeiten. Eine Umfrage des Pew Research Center ergab, dass 54 % der US-Mitarbeiter nach dem Ende der Pandemie Remote-Arbeit bevorzugen, und ein Gallup-Bericht zeigte, dass 6 von 10 Managern planen, es Mitarbeitern zu ermöglichen, häufiger remote zu arbeiten als vor der Pandemie. Aus diesen Statistiken geht hervor, dass eine zukünftige verteilte Belegschaft bedeutet, dass IT-Teams weiterhin Endpunkte physisch außerhalb von Unternehmens-Firewalls verwalten und schützen werden. Konvergente Plattformen wie Tanium, die IT-Teams Transparenz, Kontrolle und vertrauenswürdige Daten liefern, werden in einer hybriden Arbeitsumgebung weiterhin von größter Bedeutung sein.

Zweitens wird sich auch die Cloud-Migration weiterentwickeln und sensible Daten dem Risiko aussetzen, dass auf sie zugegriffen wird und sie falsch gehandhabt werden. Allein im Jahr 2022 werden die Ausgaben der Endbenutzer für Cloud-Services laut Gartner voraussichtlich um 22 % steigen. Und die Cloud ist beliebt: Der jährliche „State of the Cloud Report" ergab, dass 90 % der Unternehmen bis Ende 2022 auf eine Art von Hybrid-Cloud-Lösung angewiesen sein werden. Langfristig prognostiziert Gartner bis 2026, dass die Cloud-Ausgaben mindestens 45 % aller IT-Ausgaben für Unternehmen ausmachen werden. Daher benötigen Unternehmen Lösungen wie Tanium, die cloud-freundlich sind und einen sicheren Betrieb ermöglichen, da sie von lokalen Lösungen migrieren.

Drittens werden künstliche Intelligenz (KI) und auf maschinellem Lernen basierende Algorithmen (ML) in der Endpunktwelt nur noch wichtiger werden. Die Anpassung von Sicherheitsrichtlinien und -rollen an einzelne Benutzer in Echtzeit, basierend auf Gerätetyp, Gerätekonfiguration, Mustern dafür, wann und wo sie versuchen sich anzumelden, und anderen Variablen, ist von entscheidender Bedeutung. Tanium kann echte KI/ML in die Lage versetzen, Benutzer über verdächtiges Verhalten zu informieren und die Behebung aufgrund der Qualität der Daten, auf die es Zugriff hat, zu automatisieren – und die Geschwindigkeit, mit der es diese Daten zurückgeben kann. Unternehmen werden weiterhin in Lösungen wie Tanium investieren, die Bedrohungen kontinuierlich automatisieren, anpassen und aus ihnen lernen.

Die Converged Endpointmanagement Plattform von Tanium ist so positioniert, dass sie von diesen zukünftigen Trends profitiert.

Mit Tanium haben Kunden einen konvergenten Satz von Modulen für alles, was auf einem Gerät zur Funktion und Leistung benötigt wird. Das Konvergieren von Tools über die IT-Operations, Security und Risk und Compliance hinweg bringt Teams zusammen: eine Plattform für vollständige Visibilität, Kontrolle und Vertrauen in ihre IT-Infrastruktur.

Tanium baut seine Plattform bewusst mit Zielsetzung auf, IT-Teams (Operations und Security) zu ermöglichen, ihre Arbeit zu erledigen. Angesichts einer ständig wachsenden Angriffsfläche können IT-Führungskräfte von reaktiver Problemlösung zu proaktivem Handeln wechseln. Ihre Teams sind besser in der Lage, miteinander zu kommunizieren, während sie sich auf denselben Datensatz und dieselben Tools beziehen; es ist keine zusätzliche Schulung zwischen den Teams erforderlich; und es ist einfach, mehr Module hinzuzufügen, da jedes einzelne einfach ein Workflow ist, der auf derselben zugrunde liegenden Plattform basiert. Teams müssen weniger Anwendungen und Tools verwalten und gleichzeitig durch eine bessere Zusammenarbeit positive Auswirkungen auf die Geschäftsergebnisse erzielen.

Im Kern ist Tanium ein Datenunternehmen, das der IT hilft, zu skalieren, indem es die Welt der IT-Operations, der Security sowie der Risk und Compliance in einer einheitlichen Lösung vereint. Das ist die Power of Certainty.

Referenzen

https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf

https://venturebeat.com/2021/09/26/digital-transformation-spending-is-up-to-700b-per-year-but-results-lag/

https://federalnewsnetwork.com/federal-insights/2021/04/what-the-pandemic-driven-increase-in-it-complexity-means-for-federal-agencies/

https://www.retaildive.com/news/76-of-cios-say-it-complexity-makes-it-impossible-to-manage-performance/516065/

https://hbr.org/2021/10/does-your-team-really-need-another-digital-tool

https://www.businesswire.com/news/home/20170918005033/en/Information-App-Overload-Hurts-Worker-Productivity-Focus

https://securityboulevard.com/2021/06/proliferation-of-devops-tools-introduces-risk/

https://www.advsyscon.com/blog/break-down-silos-in-it/

https://blog.trello.com/tips-to-improve-cross-team-collaboration

https://www.beezy.net/blog/too-many-tools

https://jfrog.com/devops-tools/what-is-devsecops/

https://www.dynatrace.com/news/blog/top-eight-devsecops-trends/

https://www.maltego.com/blog/tackling-tool-fatigue-soc-teams-need-interoperable-tools/

https://explodingtopics.com/blog/remote-work-trends

https://www.parallels.com/blogs/ras/green-it-cloud-predictions-2022/#:~:text=Gartner%20forecasts%20a%20rapid%20global,enterprise%20IT%20spending%20by%202026

https://workforceinstitute.org/workers-globally-wish-for-better-technology/

https://www.formstack.com/resources/blog-software-interoperability#:~:text=The%20term%20%E2%80%9Csoftware%20interoperability%E2%80%9D%20refers,behind%2Dthe%2Dscenes%20coding

https://www.darkreading.com/edge-articles/security-considerations-in-a-byod-culture

https://site.tanium.com/rs/790-QFJ-925/images/WP-Visibility-Gap-2020.pdf

https://www.globenewswire.com/news-release/2021/05/04/2222642/0/en/GitLab-s-Fifth-Annual-Global-DevSecOps-Survey-Reveals-2020-Was-Catalyst-for-DevOps-Tool-Adoption.html